



HAL
open science

Designing a Customisable Communication System for Situation Awareness in Rescue Operations

Samer Chehade

► **To cite this version:**

Samer Chehade. Designing a Customisable Communication System for Situation Awareness in Rescue Operations. Networking and Internet Architecture [cs.NI]. Université de Technologie de Troyes, 2021. English. NNT : 2021TROY0007 . tel-03808741

HAL Id: tel-03808741

<https://theses.hal.science/tel-03808741>

Submitted on 10 Oct 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Thèse
de doctorat
de l'UTT

Samer CHEHADE

Designing a Customisable Communication System for Situation Awareness in Rescue Operations

Champ disciplinaire :
Sciences pour l'Ingénieur

2021TROY0007

Année 2021



THESE
pour l'obtention du grade de
DOCTEUR
de l'UNIVERSITE DE TECHNOLOGIE DE TROYES
en SCIENCES POUR L'INGENIEUR
Spécialité : SYSTEMES SOCIOTECHNIQUES

présentée et soutenue par

Samer CHEHADE

le 9 février 2021

**Designing a Customisable Communication System
for Situation Awareness in Rescue Operations**

JURY

M. Pascal SALEMBIER	PROFESSEUR UTT - HDR	Président
M. Frédéric BÉNABEN	PROFESSEUR IMT - HDR	Rapporteur
M. Hedi Mohamed KARRAY	MAITRE DE CONFERENCES - HDR	Rapporteur
M. Antonio DE NICOLA	DOTTORATO DI RECERCA	Examineur
M. Rémi COGRANNE	MAITRE DE CONFERENCES	Directeur de thèse
Mme Nada MATTA	PROFESSEURE UTT - HDR	Directrice de thèse

Personnalité invitée

M. Jean-Baptiste POTHIN DOCTEUR

Dedicated to my mother Fatmé and to the memory of my father Mohamad

Acknowledgements

Completing my Ph.D. has been one of the most significant academic challenges that I ever had to face, but provided me a remarkable experience. Accomplishing this academic challenge would not have been possible without many people, not only for their contributions to scientific knowledge, but also for my personal benefit from the privilege of working alongside them during this journey. These lines are dedicated to all of them.

First and foremost, I would like to thank the DataHertz team who has provided me with a magnificent professional working environment that allowed me to develop my competences all along the period of this thesis. I would particularly like to thank **Jean-Baptiste Pothin**, the head of the Research and Development department, who has warmly welcomed me to his service, has fully involved me in this project and has shared his expertise with me on a daily basis. The trust he has put in me, the level of responsibility he has allowed me to take and the time he has devoted for my thesis are things that I will always be grateful for.

My advisor **Nada Matta** does not deserve only my thanks, but also direct credit for some of the work this thesis represents. In fact, much of the intellectual work of this thesis took place in conversations with her. Nada has not just been a great advisor, but a great friend as well. I am very grateful for her patience, motivation, and immense knowledge in the field, which made this thesis as successful as it is. I would also like to thank my second advisor **Remi Cogramne**, who has always been guiding me in the right direction. His excellent research skills are one of a kind, allowing me to work on a high professional level. I simply could not wish for better advisors.

I would like to thank the reviewers **Hedi Karray** and **Frederick Benaben**, and the committee members **Antonio De Nicola** and **Pascal Salembier** for their careful reading of my thesis and the comments they addressed me during the defense in order to improve my work.

The monitoring committee that has followed me during these years, has had an important positive impact on the quality of the work achieved in this thesis. The constructive remarks and the detailed follow-up provided by its members have allowed me to continuously enhance my work to meet their high set standards. I thank the monitoring committee members in particular the external member **Hedi Karray** who gave me continuous and important advices that helped to improve our work significantly.

I also thank the doctoral school of the University of Technology of Troyes, in particular the director **Khemais Saanouni**, and the secretaries **Pascale Denis**, **Isabelle Leclercq** and **Thérèse Kazarian**.

I would also like to take the opportunity to thank my friends and colleagues for their support during the last three years. Special thanks go to my friends Dona-Elisa, Daniel, Abed, Fadel, Oussama, Ahmad, and Hussein.

My biggest thank go, without question, to my family, for Fatmé, Farah, Hicham, Wissam, and Hilal for their support and their help during these years.

Abstract

This thesis deals with the problem of awareness and communications in rescue operations. We look forward to designing and implementing a communication system aiming to simplify information sharing in rescue operations based on semantic representation techniques and a customisation of uses. In order to be used by operational units, it is essential to design such a system in a way that meets their practical needs. Moreover, in order to guarantee the privacy of information, it is essential to integrate security techniques in the proposed system. In this consequence, we propose in this thesis a novel approach for defining and designing the system's interfaces and specifications. This approach consists of a five-step methodology. First, we analyse and model communications and interactions between different stakeholders based on practical operations. Secondly, we formalise those interactions and knowledge through an application ontology. This ontology integrates concepts related to the rescue domain, to the design of systems and to information security. Afterwards, we present ontology-based platform for designing the system. Based on the developed ontology, this platform will allow the end-users of the system to define its specifications and design its interfaces in a customised way. Moreover, we propose an access control and rights management policy based on the proposed ontology. Eventually, we present a use case scenario of the proposed platform.

Keywords:

- Disaster relief
- Knowledge representation (Information theory)
- Electronic data processing departments–Security measures
- Awareness
- System design

Résumé

Cette thèse porte sur le problème d'*awareness* et des communications dans les opérations de secours. Nous cherchons à concevoir et à mettre en œuvre un système visant à simplifier les communications dans ces opérations en se basant sur des techniques de représentation sémantique et une personnalisation des usages. Pour être utilisé par les unités opérationnelles, il est essentiel de concevoir un tel système de manière à répondre à leurs besoins. De plus, afin de garantir la confidentialité des informations, il est essentiel d'intégrer des techniques de sécurité. Pour aborder ces aspects, nous proposons une approche pour concevoir les interfaces et les spécifications du système. Cette approche consiste en une méthodologie basée sur cinq étapes. Tout d'abord, nous modélisons les interactions entre les différentes parties sur la base de pratiques opérationnelles. Deuxièmement, nous formalisons ces interactions et connaissances à travers une ontologie d'application. Cette ontologie intègre des concepts liés au domaine du secours, à la conception de systèmes et à la sécurité de l'information. Ensuite, nous présentons une plate-forme pour concevoir le système. Basée sur l'ontologie développée, cette plateforme permettra aux utilisateurs finaux du système de définir leurs spécifications et de concevoir leurs interfaces de manière personnalisée. De plus, nous proposons une politique de contrôle d'accès basée sur l'ontologie proposée. Finalement, nous présentons un cas d'usage de la plateforme proposée.

Mots-clés :

- Secours aux victimes de catastrophes
- Représentation des connaissances
- Systèmes informatiques – Mesures de sûreté
- Prise de conscience
- Systèmes, Conception de



Table of Contents

List of Figures	xv
List of Tables	xix
List of Abbreviations	xxi
1 Introduction	1
1.1 Research Context	2
1.2 Rescue Overview and History	3
1.3 Problem Formulation	5
1.4 Research Questions, Solutions, and Methodology	8
1.5 Content Organisation	12
2 Communication and Situation Awareness	17
2.1 Introduction	18
2.2 Theory of Awareness	18
2.2.1 Definitions and types of awareness	18
2.2.2 Situation awareness	21
2.2.3 Situation awareness in rescue operations	25
2.2.4 Mechanisms for supporting situation awareness	26
2.3 Information Communication	28
2.3.1 Theory of information communication	29
2.3.2 Communication problems in rescue operations	31
2.3.3 Communication and information exchange models for rescue operations and emergency response	35
2.4 Awareness and communication-support systems for rescue and emergency actors	37

TABLE OF CONTENTS

2.4.1	Stakeholders' practical needs	38
2.4.2	Criteria and requirements for a usable awareness and communication-support system	40
2.4.3	Analysis of some existing systems for supporting awareness and communication	43
2.4.3.1	Organisational, spatial, and situational information exchange systems	43
2.4.3.2	Medical information exchange systems	45
2.4.3.3	Medical, organisational, spatial, and situational information exchange systems	46
2.4.3.4	Discussion and research gaps	48
2.5	Conclusions	48
3	Knowledge Representation and Ontologies	53
3.1	Introduction	54
3.1.1	Historical Background and Definition of Knowledge	55
3.1.2	Knowledge Representation	57
3.2	Ontology	60
3.2.1	Definitions	60
3.2.2	Ontology categories and constituents	64
3.2.3	Ontology languages	67
3.2.4	Ontology development methodologies	68
3.3	Existing Ontologies	70
3.3.1	Ontologies for rescue and emergency response	70
3.3.2	Ontology-based approaches for designing systems and interfaces	76
3.3.3	Ontology-based approaches for access control and rights management	80
3.4	Conclusions	85
4	Modelling Interactions	89
4.1	Introduction	90
4.2	Rescue Operations in French Context	91
4.2.1	Involved organisations and actors	91
4.2.2	Organisational Model	94
4.2.3	Scenario of a rescue operation	96
4.3	Modelling Interactions and Communications	99

TABLE OF CONTENTS

4.3.1	Requirements for modelling interactions	99
4.3.2	Rescue operation chronology	101
4.3.3	Structural model	103
4.3.4	Interaction model	105
4.4	Conclusions	118
5	ResOnt Ontology	121
5.1	Introduction	122
5.2	Proposed solutions	123
5.3	Methodology of Ontology Development	125
5.3.1	Specification	128
5.3.1.1	Ontology purpose	128
5.3.1.2	Competency Questions	128
5.3.1.3	Knowledge acquisition	130
5.3.2	Conceptualisation	132
5.3.2.1	ResOnt modules	132
5.3.2.2	Reused ontologies	134
5.3.3	Formalisation and implementation	139
5.3.4	Evaluation	141
5.3.5	Maintenance	142
5.4	ResOnt Ontology Description	143
5.4.1	ResOnt Rescue and Communication Module	143
5.4.2	ResOnt Design Module	146
5.4.3	ResOnt Access Control Module	149
5.4.4	Complete ResOnt Ontology	151
5.5	Conclusions	155
6	A New Secured Platform for Rescue Situation Awareness and Communications	157
6.1	Introduction	159
6.2	Basic Principles	160
6.3	MODES Platform Functionalities and Architecture	163
6.3.1	Main functionalities	163
6.3.2	Platform Architecture	165
6.3.3	Data flow	167
6.4	Context Identification	168
6.4.1	Context creation	169

TABLE OF CONTENTS

6.4.2	Task creation	172
6.5	Dynamic and customised system and interface design	176
6.5.1	Specification configuration	178
6.5.2	Template creation	182
6.6	Communication and Access Control	187
6.6.1	User authentication	188
6.6.2	Connexion to intervention and context selection	189
6.6.3	Access Control and Rights Management	191
6.6.3.1	Rights management	198
6.6.3.2	Permissions control	201
6.6.4	Information reception and consulting	211
6.6.5	Transmission of information	212
6.7	Discussion	214
6.8	Conclusions	214
7	Experimentations	219
7.1	Introduction	220
7.2	Platform Implementation	220
7.3	System Design	227
7.3.1	Configuration of specifications	227
7.3.2	Design and templates creation	230
7.3.2.1	Case of Commander of rescue operation	232
7.3.2.2	Case of CTA Operator	233
7.3.2.3	Case of CIS Operator	235
7.4	Scenario of incident	238
7.4.1	Scenario description	238
7.4.2	Communication based on the scenario described	239
7.5	Conclusions	246
8	Conclusions	249
8.1	General Conclusion	250
8.2	Limitations and Perspectives	255
A	Résumé de la thèse	259
A.1	Introduction	261
A.1.1	Questions de recherche, solutions, et méthodologie	262
A.1.2	Contributions	266

TABLE OF CONTENTS

A.2	Communication d'information	267
A.2.1	Modèles de communication pour le secours à personne . . .	267
A.2.2	Systèmes de support à la communication	267
A.3	Ontologies et représentation des connaissances	268
A.3.1	Définitions	269
A.3.2	Méthodologies de construction des ontologies	269
A.3.3	Ontologies pour le secours et la gestion des urgences	271
A.3.4	Approches et ontologies pour la conception de systèmes et d'interfaces	272
A.3.5	Approches et ontologies pour le contrôle d'accès	272
A.4	Modélisation des interactions	274
A.4.1	Secours à personne en France	274
A.4.2	Modèle organisationnel	275
A.4.3	Modélisation des interactions et des communications	276
A.4.3.1	Exigences pour la modélisation des interactions	276
A.4.3.2	Modèle d'interactions dans le secours	277
A.5	Ontologie ResOnt	279
A.5.1	Méthodologie de développement	280
A.5.1.1	Spécification	281
A.5.1.2	Acquisition de connaissances	281
A.5.1.3	Conceptualisation	282
A.5.1.4	Formalisation et implémentation	283
A.5.1.5	Évaluation	283
A.5.1.6	Maintenance	284
A.5.2	Description de l'ontologie ResOnt	284
A.5.2.1	Module ResOnt Rescue and Communication	284
A.5.2.2	Module ResOnt Design	285
A.5.2.3	Module ResOnt Access Control	286
A.5.2.4	Ontologie ResOnt complète	286
A.6	Plateforme de support à l'awareness	288
A.6.1	Principes de base	288
A.6.2	Fonctionnalités et architecture	290
A.6.3	Identification du contexte	291
A.6.4	Configuration et conception dynamiques et personnalisées	293
A.6.5	Communication et contrôle d'accès	294
A.6.5.1	Authentification et sélection du contexte et d'intervention	294

TABLE OF CONTENTS

A.6.5.2	Contrôle d'accès et gestion des droits	294
A.6.5.3	Réception et transmission d'information	296
A.7	Expérimentations	296
A.8	Conclusions et perspectives	298
A.8.1	Conclusion générale	298
A.8.2	Perspectives	299
	Bibliography	303

List of Figures

1.1	Methodology steps for designing a customised communication system that guarantees confidential access to information.	11
1.2	Overview of the thesis structure and correlation of chapters. . . .	13
2.1	Types of awareness in group work.	20
2.2	Model of situation awareness in dynamic decision making.	22
2.3	Interactive sub-systems approach to situation awareness.	24
2.4	General communication model.	29
2.5	Information flow and complexity in rescue operations.	34
3.1	Hierarchy of data, information, and knowledge.	57
3.2	Ontologies classification based on domain scope.	64
4.1	Distribution of operational activity by categories.	92
4.2	Composition of a SDIS: Centres and services.	93
4.3	Composition of a SAMU: Centres and services.	94
4.4	Hierarchical tree of command and general flow of information and decisions.	95
4.5	Process of a medical rescue operation.	97
4.6	Chronology of phases and sub-phases in rescue operations.	101
4.7	Interactions structure model.	104
4.8	Interactions during the alert phase.	106
4.9	Interactions during the involvement of required resources (1). . . .	107
4.10	Interactions during the involvement of required resources (2). . . .	108
4.11	Interactions during the departure of rescuers (1).	109
4.12	Interactions during the departure of rescuers (2).	110
4.13	Interactions during On-site operations (1).	110
4.14	Interactions during On-site operations (2).	111

LIST OF FIGURES

4.15	Interactions during On-site operations (3).	111
4.16	Interactions during On-site operations (4).	112
4.17	Interactions during Victim’s transportation (1).	114
4.18	Interactions during Victim’s transportation (2).	115
4.19	Interactions during the return and end phase (1).	116
4.20	Interactions during the return and end phase (2).	117
5.1	Methontology steps for ontology construction.	127
5.2	Different modules of ResOnt Ontology.	133
5.3	BFO 2.0 is-a hierarchy.	135
5.4	CCO Ontologies and importation structure.	137
5.5	Different modules and alignment of ResOnt Ontology.	139
5.6	Metrics and specifications of ResOnt ontology.	140
5.7	Is-a hierarchy of the ResOnt Rescue and Communication Module.	146
5.8	Is-a hierarchy of the ResOnt Design Module.	148
5.9	Is-a hierarchy of the ResOnt Access Control Module.	150
5.10	Conceptual graph related to communications and practices.	151
5.11	Conceptual graph related to the design of systems and interfaces.	152
5.12	Conceptual graph related to access control and rights management.	153
6.1	Basic principles of the proposed solution.	161
6.2	General Architecture of the proposed platform.	165
6.3	Use case diagram for context identification.	168
6.4	Sequence diagram for context creation.	170
6.5	SPARQL Query for retrieving different phases based on a specific organisation member role.	171
6.6	Selection of phase, sub-phase, and location in MODES platform.	172
6.7	Selection of communication instrument in MODES platform.	172
6.8	Task creation section in MODES platform.	173
6.9	Sequence diagram for task creation.	174
6.10	Creation of task in a given context in MODES platform.	175
6.11	Configuration of a created task in MODES platform.	175
6.12	Summary of contextual groups of information and information elements.	176
6.13	Use case diagram for dynamic configuration and customised design.	177
6.14	Sequence diagram for configuration of specifications.	179
6.15	SPARQL Query for retrieving different information, properties, and possible values for a group of information.	180

LIST OF FIGURES

6.16	Configuration of specifications in MODES platform.	181
6.17	Sequence diagram for template creation.	183
6.18	Creation of template in MODES Platform.	185
6.19	Positioning of components and integration of media components in MODES Platform.	186
6.20	Use case diagram for MODES communication system.	187
6.21	Sequence diagram for user authentication.	189
6.22	Sequence diagram for intervention and context selection.	190
6.23	Illustration of Core components from TT-RBAC and interaction between them.	193
6.24	Access control model based on adapted TT-RBAC.	195
6.25	Use case diagram for Access Control and Rights Management. . .	197
6.26	SPARQL Query for deleting existing access rights.	201
6.27	SPARQL Query for inserting the relation <i>Has No Access On</i> be- tween a role and a group of information.	201
6.28	Sequence diagram for permissions control in MODES platform. . .	205
6.29	Sequence diagram for information reception and consulting.	211
6.30	Sequence diagram for information transmission.	212
7.1	Components and technologies in the developed platform.	222
7.2	Three created modules in the developed platform.	227
7.3	Possible values of the informational components in the platform. .	228
7.4	Possible values of the field type in the platform.	228
7.5	Configuration of specifications for the information entitled <i>Address</i> . .	229
7.6	Configuration of specifications for the information entitled <i>Incident</i> . .	229
7.7	Configuration of specifications for the information entitled <i>Time</i> . .	230
7.8	Phases, sub-phases, and roles considered in the example.	231
7.9	Configuration of context elements for a CRO.	232
7.10	Selection of Smartphone in a context for CRO.	232
7.11	Creation of task associated with CRO.	232
7.12	Partial view of the template created for the CRO before modification. .	233
7.13	Partial view of final template designed for the CRO.	234
7.14	Context and tasks created for the CTA Operator.	235
7.15	Template created for the CTO Operator before modification. . . .	236
7.16	Final template designed for the CTA Operator.	236
7.17	Template designed for the CIS Operator during the sub-phase <i>Re-</i> <i>ception of departure ticket in CIS</i>	237

LIST OF FIGURES

7.18	Template designed for the CIS Operator during the sub-phase <i>Warning rescuers</i>	237
7.19	Selection and connexion to an intervention by the CTA Operator.	240
7.20	Selection of the context created for the CTA Operator.	240
7.21	Graphical interface for the CTA Operator in the selected context.	241
7.22	Fulfilment of call information in the system by the CTA Operator.	241
7.23	Fulfilment and transmission of groups that compose the departure ticket by the CTA Operator.	242
7.24	Reception of groups that compose the departure ticket by the CIS Operator.	243
7.25	Transmission of different groups that compose the departure ticket to the involved actors.	244
7.26	Reception of groups that compose the departure ticket by the CRO.	244
7.27	Deletion of the group <i>Incident Information</i> by the CRO.	245
A.1	Méthodologie pour concevoir un système de communication personnalisé qui garantit la confidentialité des informations.	265
A.2	Hiérarchie du module ResOnt Rescue and Communication.	285
A.3	Hiérarchie du module ResOnt Design.	286
A.4	Hiérarchie du module ResOnt Access Control.	287
A.5	Graphe conceptuel lié aux communications et aux pratiques.	287
A.6	Graphe conceptuel lié à la conception de systèmes et d'interfaces.	288
A.7	Graphe conceptuel lié au contrôle d'accès et à la gestion des droits.	289
A.8	Architecture générale de la plateforme proposée.	292

List of Tables

2.1	Main groups of information and information elements required by participating actors in rescue operations.	32
2.2	Communication and interaction models for rescue operations and emergency response.	36
2.3	Awareness and communication-support systems and their classification according to stakeholder' needs.	49
2.4	Awareness and communication-support systems and their classification according to identified systems criteria.	50
3.1	Existing ontologies for rescue, emergency response, and crisis management domains.	74
3.2	Existing ontologies for systems and interfaces design.	81
3.3	Existing ontologies for access control and rights management.	85
5.1	Comparison of ontologies development methodologies against the ontology development life cycle.	126
5.2	Competency questions related to practices and interactions in rescue operations.	129
5.3	Competency questions related to the design of the system and interfaces.	131
5.4	Competency questions related to access control and rights management.	131
5.5	Definitions of BFO's meta-classes.	136
5.6	Classes and relations of ResOnt Ontology.	141
5.7	Comparison of ResOnt to other existing ontologies in rescue and emergency response domain according to considered aspects.	154
5.8	Comparison of ResOnt to other existing ontologies related to systems and interface design according to considered aspects.	154

LIST OF TABLES

5.9	Comparison of ResOnt to other related to access control and rights management according to considered aspects.	154
6.1	SWRL Rules for determining the relation between an organisation member role and a group of information in terms of access rights.	200
6.2	Comparison of MODES to other existing systems according to stakeholder' needs.	215
6.3	Comparison of MODES to other existing systems according to the criteria for an effective communication system.	216

List of Abbreviations

SAR	Search and Rescue
SDIS	Service Départemental d’Incendie et de Secours (Local Services for Fire and Rescue)
SAMU	Service d’Aide Médicale Urgente (Urgent Medical Assistance Services)
CSCW	Computer Supported Cooperative Work
AI	Artificial Intelligence
DOLCE	Descriptive Ontology for Linguistic and Cognitive Engineering
SUMO	Suggested Upper Merged Ontology
BFO	Basic Formal Ontology
XML	eXtensible Markup Language
RDF	Resource Description Framework
OWL	Ontology Web Language
DAML	DARPA Agent Markup Language
OIL	Ontology Inference Layer
SWRL	Semantic Web Rule Language
AFM	Activity First Methodology

LIST OF ABBREVIATIONS

TOVE	Toronto Virtual
UPON	Unified Process for Ontology Building
UP	Unified Process
UML	Unified Modelling Language
EDXL	Emergency Data Exchange Language
IDA	Institute for Defence Analyses
BFiaO	Basic formal infrastructure incident assessment ontology
CESAR	Coordination of Emergencies and Tracking of Actions and Resources
BFER	Building Fire Emergency Response
CROnto	Crisis Response Ontology
EMO	Emergency Response Ontology
MOAC	Management of a Crisis Vocabulary
UI	User Interface
UIO	User Interface Ontology
GUI	Graphical User Interface
EUD	End User Development
AC	Access Control
RBAC	Role-Based Access Control
TMAC	Team-Based Access Control
ABAC	Attribute-Based Access Control
XACML	eXtensible Access Control Markup Language
AMO	Access Management Ontology

Or-BAC	Organisation-Based Access Control
ORSEC	Organisation de la Response de Sécurité Civile
CTA	Centre de Traitement de l’Alerte (Call Processing Centre)
CIS	Centre d’Incendie et de Secours (Fire and Rescue Centre)
CODIS	Centre Opérationnel Départemental d’Incendie et de Secours (Departmental Emergency Operations Center)
SSSM	Service de Santé et de Secours Médical (Health and Medical Rescue Service)
CRRA	Centre de Réception et de Régulation des Appels (Call Reception and Dispatch Centre)
SMUR	Structure Mobile d’Urgence et de Réanimation (Mobile Service of Emergency and Reanimation)
FIPA	Foundation for Intelligent Physical Agents
CRO	Commander of Rescue Operation
CQs	Competency Questions
MILO	Mid-Level Ontology
RO	Relation Ontology
ER	Emergency Response
JWT	JSON Web Token
DAC	Discretionary Access Control
MAC	Mandatory Access Control
IBAC	Identity Based Access Control
RBAC	Role Based Access Control
TMAC	TeaM Based Access Control

0. LIST OF ABBREVIATIONS

TBAC	Task Based Access Control
T-RBAC	Task-Role Based Access Control
TT-RBAC	Team and Task Based RBAC
DOM	Document Object Model

Chapter 1

Introduction

Contents

1.1	Research Context	2
1.2	Rescue Overview and History	3
1.3	Problem Formulation	5
1.4	Research Questions, Solutions, and Methodology . .	8
1.5	Content Organisation	12

1.1 Research Context

In his lifetime, each person is exposed to pass through distress situations due to particular events. Whether they are of small-scale such as car accidents and trauma or of large-scale like natural disasters or terrorist attacks, these events require responsive operations called rescue operations. Rescue operations, also called Search and Rescue Operations (SAR), consist in saving properties and victims' lives and by involving public organisations as well as private ones. In France, many public services are involved in such operations. They have to protect victims by ensuring their safety, securing the surroundings, providing first aids, and arranging transportation and evacuation to a relevant place of reception [Diederichs *et al.*, 2006]. Rescuers from various organisations have to collaborate with each other in order to achieve successful operations. Moreover, a high level of situation awareness is required amongst those rescuers in a way that each participant can be aware of the situations and activities of others despite the location of each one. The term "Collaboration", which comes from the Latin "Collaborare" (co "with"; laborare "to work") implies working in "a group of two or more people to achieve a common goal while respecting the contribution of each individual to the whole" [McInnerney & Roberts, 2009]. Moreover, according to the Cambridge English Dictionary, the term "Awareness" means "knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience" [Crystal, 2004]. This term consists in knowing what is going on around in order to integrate and complete its activities [Schmidt, 2002]. This means that actors need to perceive and understand the situations in order to act. Hence, effective communication is required between different participants in order to reach high levels of collaboration and situation awareness. However, the ability to gather quickly, fuse and exchange relevant information is challenging in complex and dynamic domains such as the rescue and emergency response domains. An enormous information flow has to be managed and most of the decisions are made based on this information. This complexity and information flow may lead to inefficient interactions between different actors, which can influence collaboration and situation awareness. Authors in [Saoutal *et al.*, 2014] reported that ineffective communication between actors can lead to misunderstanding and misinterpretation of a situation, which can cause a lack of awareness about it and affect victims' safety. Assessments from many real incidents underline challenges of unsuccessful information exchange between engaged responders and their consequences on the operations' outcomes. For

example, concluding reports on the terrorist attacks on November 13, 2015, in France, revealed major communication issues between different services. According to this report, each service focused on its own information and several victims on two different sites were not evacuated on time due to a lack of coordination [Fenech & Pietrasanta, 2016]. Consequences of communication problems are not limited to those regarding the victims' lives. In some cases, these problems can threaten the actors themselves. For example, on September 4, 2018, a French firefighter was killed in Paris by an unstable victim during his evacuation. The reason behind this accident was a lack of communication between medical services and firefighters: "During the call transfer, medical services did not provide sufficient information about the seriousness of the situation" stated the firefighters chief [Décugis & Pelletier, 2018].

Several systems aiming to support awareness have been proposed in the context of emergency response and rescue operations. Unfortunately, recent studies reveal persistent awareness problems in those domains [Munkvold *et al.*, 2019; Steen-Tveit & Radianti, 2019]. Therefore, an essential need for supporting communications in rescue operations can be underlined as a primary requirement toward enhancing situation awareness amongst different participating actors. Those enhancements will surely help to improve actors' reactions and activities and thus operations' outcomes. In this thesis, we focus our study on daily rescue operations that imply the participation of firefighters and medical services. Our main objective is to provide a solution to awareness problems in daily response operations in France. However, the work presented does not cover large-scale and disaster response operations.

1.2 Rescue Overview and History

Man-made and natural incidents are inevitable, frequent, and can cause permanent losses. Although no emergency plans can prevent properties' destruction and lives' losses, effective rescue operations are required to lessen damages and undesirable consequences. In 2018, a total of 3394907 persons were rescued in France [French Ministry of Interior, 2019]. Those persons were victims of different events such as malaise in public or private places, home accidents, public road accidents, workplace accidents, and intoxications.

Rescue operations are defined as a set of activities that consist in searching, rescuing, and evacuating patients and victims during disasters and distress situations

1. INTRODUCTION

by private and public teams who are well-equipped and trained for supporting and helping people [Yoncaci, 2020]. Those operations incorporate several speciality sub-fields, generally determined by the type of intervention site and the terrain where operations are conducted. Those sub-fields include air-sea rescue over water, urban rescue in cities, mountain rescue, and cave rescue [Yoncaci, 2020]. One of the world's earliest reported rescue operations arose during the 1656 crash of the Dutch trader ship Vergulde Draeck off the Australian's west coast. In response to survivors seeking help, three distinct search and rescue operations were handled without success [Major, 1859]. In France, the organisation of the emergency care system and rescue domain is the result of progressive evolution. This organisation dates back to the year 803 under the reign of Charlemagne. The emperor set up the "watch", a kind of service provided at night by the bourgeois in order to prevent the plagues that could threaten them such as theft, violence, and fires [De Gaulle, 1839]. In 1811, Napoleon 1st created by decree the Corps of Firefighters in order to enhance the effectiveness of rescue efforts [Sapaut, 2011]. From 1920, the fire and rescue services were created, organised and made decisive progress. In 1938, a law provided for the creation of the Local Services for Fire and Rescue (SDIS) and the Dordogne was one of the first French departments to officially create this service in 1942. Later on, the municipal firefighters perceived more modern equipment thanks to passive defence endowments [SDIS24 France, 2017]. Efforts toward the organisation of the emergency response and rescue domain were continued by the creation of the Urgent Medical Assistance Services (SAMU) in 1986 [Glaa, 2008].

Rescue operations are characterised by the multiplicity of involved stakeholders and organisations. This multiplicity and diversity constitute a heterogeneous composition with respect to organisational structure in the intervention site. In most of the countries, involved organisations and services include the medical services, firefighters, armed forces, police departments, and in some cases multiple additional organisations such as non-governmental organisations like red-cross or civil protection [Pužar, 2010]. For example, in Norway, police departments have the primary duty for managing intervention sites and coordinating between different involved organisations, as well as public authorities represented by governmental departments and the county governor who might get involved in some large-scale events. Each organisation has its practices and procedures. Moreover, coordination structure and procedures regarding inter-organisational interaction are defined in order to achieve successful operations. Those procedures and interactions are also extended to the description of the information flow between

different organisations, even though this flow might, in some cases, vary during the operations [Pužar, 2010].

1.3 Problem Formulation

The problem addressed in our work is situation awareness in a complex and dynamic domain that is the domain of rescue. We especially addressed effective information sharing as a first brick towards helping this awareness, the first key factor for success in rescue and emergency response operations. In most of the countries, concluding reports from the majority of incidents pointed out persisting collaboration problems and communication difficulties [Comfort *et al.*, 2004; Elmhadhbi, 2020; Martin *et al.*, 2016; Nowell & Steelman, 2015]. For example, after-actions reports from the Paris terrorist attacks stated that the firefighters and emergency medical services faced serious difficulties in communication and coordination of their efforts [Fenech & Pietrasanta, 2016]. These problems were also highlighted in the 9/11 attacks in the United States. This is due to six main reasons. First, communication during rescue and emergency response operations is still limited to oral communication using radio devices. Radio communications might cause serious problems due to the use of different frequencies by distinct involved services. According to [Roger & Martin, 2018], during the Weybourne (Norfolk) leaking container ship incident, coastguards, police, and firefighter units highlighted their dissatisfaction with the use of radio communications during the event. Those services experienced incompatible radio systems due to a lack of common communication frequencies. In France, despite the large number of existing communication systems that are oriented for rescue actors, recent statistics show that the majority of information exchange is still oral [Mallek *et al.*, 2016]. The vice-president of the National Federation of firefighters of France, Patrick Hertgen claimed that: “The name and address are dictated over the phone, and the caller has to repeat himself. This constitutes a considerable waste of time” [Verbaere, 2013]. Second, since rescue and emergency response actors come from different backgrounds and services with different levels of expertise, they use different terminologies and semantics that are difficult to harmonise. Those actors have distinct interpretations of expressions and words. The resulting semantic heterogeneity of information and the lack of a shared interpretation of data may lead to misunderstandings between the involved actors, which may cause irrelevant decisions and actions. According to the Norwegian Ministry of Justice and

1. INTRODUCTION

Public Defence, different terminology in use by the different responders for depicting the same concepts and events represents a challenge for information sharing and shared situational understanding [Munkvold *et al.*, 2019]. Third, most of the existing communication systems are oriented for specific emergency services without considering other involved services. For example, some systems are oriented for firefighters while others are oriented for medical services. A direct result of this situation is that the information is heterogeneous; they are stored in distinct data sources with distinct forms. This heterogeneity results in a deficiency of interoperability between the existing systems and thus between different services. In 2013, the president of medical services in France, François Braun stated: “The will to communicate is there but it comes up against technical constraints. The Call processing systems between medical services and firefighters are incompatible” [Verbaere, 2013]. Fourth, in rescue operations, due to the enormous amount of generated information and the rapid evolution of events, different services may be upset and irrelevant decisions may be made. Consequently, resources are managed improperly, which may affect the victims’ lives. Different involved services collaborate together to secure victims, evacuate them, and transport them to the appropriate hospitalisation centre. Reports on Paris terrorist attacks pointed out the necessity of enhancing the resources allocations and the evacuation methods of victims to save their lives [Elmhadhbi, 2020]. Fifth, most of the rescue and emergency response services still face problems related to the exchange of different types and forms of information using the existing systems. The rescue stakeholders’ must be able to exchange different types of data whether they are operational, situational, spatial, or medical information. Moreover, they must be able to transmit and receive videos, photos, voices, and texts to enhance situational awareness. A recent study showed that a simple photo or a short video brings an incredible amount of information if they can be taken and easily transmitted by the citizen to the involved services, or from the first responder on the field to the operation centre [Lambert *et al.*, 2019]. This provides a much more accurate picture of an emergency situation, speeding up incident response times by using a multitude of potential data sources for incident command [Lambert *et al.*, 2019]. During an interview that took place in 2018, Doctor Michael Bignan, a doctor attached to the firefighters of Paris stated: “We must now take the next step with a national and unique application that allows all at the same time: the alert of the rescue services, the guidance of rescue actions, the alert of citizens in the event of crisis and increased call for help, as well as the transmission of images and video and medical data” [Bertrand, 2018]. Similarly, a

1.3 Problem Formulation

report following the 9/11 attacks suggests that well-defined requirements must be established for data, imagery, voice, video, back-up capabilities, and display functions. During the 9/11 attacks, public networks and communication systems were overwhelmed and rendered virtually ineffective and the services could not exchange different forms of data [Barthel, 2012]. Sixth, during disasters and rescue operations, gathering both timely and actionable operational and medical information is a challenge due to the paradox of information overload [Chan & Purohit, 2019]. In other words, the presence of information often does not equate to an improved awareness of the disaster environment. During the aftermath of the 2010 Haiti earthquake, for which both global and US disaster response systems activated, the growth of digital information in the form of mobile communications, web-based information systems, geographic information, and digital volunteer activity resulted in not only unprecedented large volumes of information, but also the recognition by the humanitarian community of the information ecosystem and challenges that lie ahead [Chan & Purohit, 2019]. It is therefore essential to deliver the right information to the right person at the right moment to prevent information overload problems. Unfortunately, most of the existing solutions do not account for the fact that information needs might vary depending upon an actors' role and context [Zade *et al.*, 2018].

The improvement of communication and information sharing in rescue operations has been the topic of numerous studies over the past decades. Numerous solutions have been developed attempting to solve serious problems that lead to inefficient decision-making such as lack of situation awareness and inefficiency in information sharing. In this context, several systems were developed to support information exchange, communication, and collaboration. Unfortunately, recent studies report a low adoption of communication systems in rescue operations as well as a negative position of actors to such systems [Elmasllari, 2019]. Indeed, most of the existing systems are not fully accepted by actors since they are limited to some functionalities or are developed without examining the real activities of actors. The real needs of stakeholders, simply put, are not satisfied by the offered systems. Observing this circumstance through a design focal point, we notice that such issues ordinarily originate from the use of irrelevant design techniques as well as inadequate approaches to collect and understand user preferences. Hence, a vital need for proposing a communication system that supports communications, meets stakeholders' needs and gains their acceptance and acceptability is underlined. However, designing systems for users who work in complex domains such as rescue operations is still challenging. This is due to

1. INTRODUCTION

many reasons. First, a good system design approach requires collecting all of the users' requirements and preferences in a way to propose a relevant and easy to use system. In the domain of rescue where multiple actors coming from several different organisations participate in one operation, it is difficult to respond to this requirement since users come from various backgrounds with distinct roles. This imposes offering specifications and interfaces to the user based on her/his role. The second important problem is the diversity of contexts and tasks to achieve. For instance, participant actors are in different locations with distinct tasks to achieve. The participants are supposed to receive, consult, or transmit information based on the task being handled. This causes a heterogeneity in the information to exchange depending on each context and task, which will surely complicate the design phase. Moreover, exchanged information during rescue can take several forms such as text, audio, video, signal, or graphic. This diversity requires designing the system in a way to consider these different forms. Finally, a great amount of exchanged information is of sensitive nature such as personal information related to the medical status of victims. Hence, guaranteeing the privacy of this information is mandatory. Therefore, it is of great importance to take the privacy of information into consideration in the design of the system. All of the aforementioned reasons and difficulties makes the design of communication systems for rescue actors a very challenging task.

In this thesis, we choose to support the design of communication systems for rescue actors, which will help to support communications and situation awareness.

1.4 Research Questions, Solutions, and Methodology

The research project presented in this thesis is part of the definition of a flexible system that improves information sharing, the first support for awareness in collaborative work in an emerging, complex and dynamic domain, which is the domain of rescue. This system shall be designed in a way that guarantees mutual awareness between different stakeholders. Moreover, it is essential that the system ensures effective communications and confidential access to information. In addition, it is essential that the system guarantees the exchange of actionable information based on users' contexts. In other words, it must allow its end-users to exchange the right information to the right person at the right time which will

1.4 Research Questions, Solutions, and Methodology

enhance the quality of their actions based on the information. Finally, it is of great importance to design the system in a way that gains stakeholders acceptability. Consequently, three research questions and three corresponding solutions were formulated:

Q.1: How to ensure situational awareness amongst participating actors in rescue operations?

Based on the definition of awareness, a key first step toward achieving it and reaching its highest levels consists in ensuring a common perception of situations between collaborating actors. This will enhance the decisions, performance, and users' actions. Several studies boosted the idea of the existence of solid links between perception, action, and decision-making [De Oliveira *et al.*, 2009]. Ensuring a common perception of situations ensuring require effective information exchange and communication between those actors. Moreover, unifying situations' perception requires the definition of main concepts that can represent activities of different actors. Therefore, it is essential that the proposed system helps to represent a common perception of concepts between actors. Semantic representation techniques [Sowa, 1999; Studer *et al.*, 1998] and ontologies [Gruber *et al.*, 1993] can be very helpful in order firstly to represent main situation's entities and then to guide situation's perception sharing [Nunavath *et al.*, 2013]. Therefore, the first solution consists in enhancing interactions and information exchange through a communication support system based on semantic representation techniques and ontologies.

Q.2: How to guarantee effective communications as well as confidential access to information in rescue operations?

In order to guarantee effective communications, the proposed communication system must respond to the stakeholders' needs. Those include exchanging different required types and forms of data, interoperable communications between stakeholders, common terminology, and exchange of actionable information based on different contexts. In addition, it must guarantee and support the exchange of the right information to the right person at the right time, which is referred to as the actionability [Coche *et al.*, 2019; Zade *et al.*, 2018]. It is therefore badly required to consider real practices and interactions in the design of the communication support system. Hence, it is of great importance to study, analyse, and model those interactions and practices [Saoutal, 2015]. This allows identifying the actionable information required by each person according to his/her role and

1. INTRODUCTION

context. Regarding the confidentiality aspect, adequate mechanisms and techniques must be integrated into the communication system in order to guarantee the privacy of information. In this manner, it is necessary to adapt the adequate confidentiality policies and mechanisms to the intervention needs of the rescuers. Hence, those mechanisms shall be chosen on the basis of the practices and interactions. A very well known approach that responds to this requirement is the approach of “Security by Design”, which consists in designing an information system taking into account the security of the latter from the beginning of its design design and specification [El Kalam, 2003]. Hence, the second solution relies on taking the real practices and interactions into consideration in the design phase. This solution also consists in choosing relevant confidentiality policies and mechanisms in a way that meets the stakeholders’ needs.

Q.3: How to guarantee the acceptability of the proposed system by its end-users?

Users’ acceptability is one of the basic prerequisites of any user support tool and assistive technology [Wilkinson & De Angeli, 2014]. Hence, one of the considerable challenges is that of developing technology which is acceptable and usable by end-users having different arrangement of needs, requirements, and capabilities. To ensure the users’ acceptability of the proposed system, it is crucial that this latter supports the central process and practices efficiently. Users’ acceptability can be studied through different approaches. One of these approaches is based on the system’s design and ergonomics [Alexandre *et al.*, 2018]. Similarly, there exist several approaches and methods for designing systems. Implying users in the design of the system is the best way to increase the acceptability and usability of the systems [Wilkinson & De Angeli, 2014]. We thus propose to allow the end-users of the system to define its interfaces and specifications by themselves based on their roles, tasks, and contexts. Therefore, the third solution consists in proposing a novel approach through which final users can design the system in a customised way based on a semantic representation of knowledge.

Based on the three proposed solutions, we propose to design and implement a communication system aiming to simplify information sharing based on semantic representation techniques and a customisation of uses. This system is referred to as MODES, which stands for Medical and Operational Data Exchange System. In order to be used and accepted by operational units, it is essential to design such a system in a way that meets their practical needs. Moreover, in order to guarantee the privacy of information, it is crucial to integrate the appropriate

1.4 Research Questions, Solutions, and Methodology

mechanisms in the proposed system in a way that meets the stakeholders' needs. In this context, multiple mechanisms can be integrated such as data encryption, authentication, access control, as well as other mechanisms related to the security of communication infrastructure. However, in this work, we only focus on a single aspect that is access control and rights management in the communication system since other mechanisms like data encryption can be ensured with standard tools. We propose in this thesis an approach for identifying the system's specifications and designing its interfaces by its end-users. The proposed approach includes the integration of an access control and rights management policy to guarantee the confidential access to information in the system to develop. To this end, MODES platform that allows the design of the system interfaces and specifications in a customised way is proposed. This approach consists of a five-step methodology as shown in Figure 1.1.

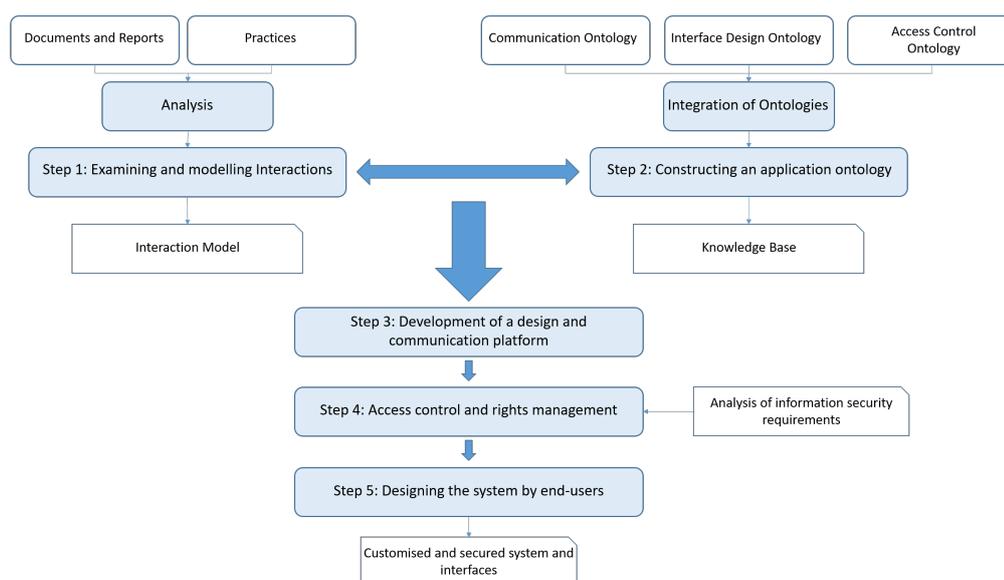


Figure 1.1: Methodology steps for designing a customised communication system that guarantees confidential access to information.

As we can see in Figure 1.1, the first step consists in examining and modelling interactions based on real practices. The importance of this step is to identify the information required by each person based on her/his role, context, and tasks to achieve. The second step relies on constructing an application ontology that represents the knowledge required for designing a communication system oriented for rescue actors that guarantees the confidentiality of information. This ontology

1. INTRODUCTION

consists of three modules. The first module is oriented for representing knowledge related to communications in rescue operations. It serves for ensuring a common interpretation of information between different stakeholders as well as representing and formalising different procedures and flow of information. The second module incorporates knowledge required for the dynamic design and configuration of the system and interfaces. Whereas, the third module is specific for guaranteeing access control management in the system. In order to manipulate the processing of different inferences, it is important to define relations between different concepts and instances based on real interactions. Hence, the first and the second steps are interdependent between them. The third step consists in developing MODES, an ontology-based platform for design and communication. Based on the previously developed ontology, this platform will allow the end-users of the system to define its specifications and design its interfaces in a customised way. The importance of using an ontology in this step is to develop a flexible platform that allows the dynamic configuration of system. Regarding the fourth step, it lies within integrating confidentiality mechanisms in the system. As being said above, we focus in this thesis on the access control mechanism. In this context, we propose an access control and rights management policy to guarantee the confidential access to information in the system based on the developed ontology. Whereas, the fifth step consists in designing the system's specifications and interfaces by its end-users in a customised through the proposed platform. The aim of passing through these steps is to propose a personalised, usable, and flexible system that guarantees the confidentiality of information and can be accepted by the stakeholders.

1.5 Content Organisation

This thesis tackles the problem of awareness and communication in rescue operations and proposes several contributions in the domain. The main contribution is the proposal of an approach and a platform for designing a communication system oriented for French rescue actors. First, we model interactions between actors and identify modelling requirements. Second, we present an application ontology, called ResOnt, developed to represent and formalise the knowledge for designing a communication system oriented for rescue and emergency response actors that guarantees the confidentiality of information. This ontology consists of three modules. The first module is oriented for representing knowledge related

to communications in rescue operations. The second module incorporates knowledge required for the design of the system and interfaces. Whereas, the third module is specific for guaranteeing access control management in the system. Finally, we present MODES platform that allows users to identify and design the system’s specifications and interfaces in a customised way using the described interaction model and the proposed ontology. Following this design step, end-users will be able to communicate effectively in rescue operations.

Organisation of the manuscript

The organisation of the manuscript is shown in Figure 1.2.

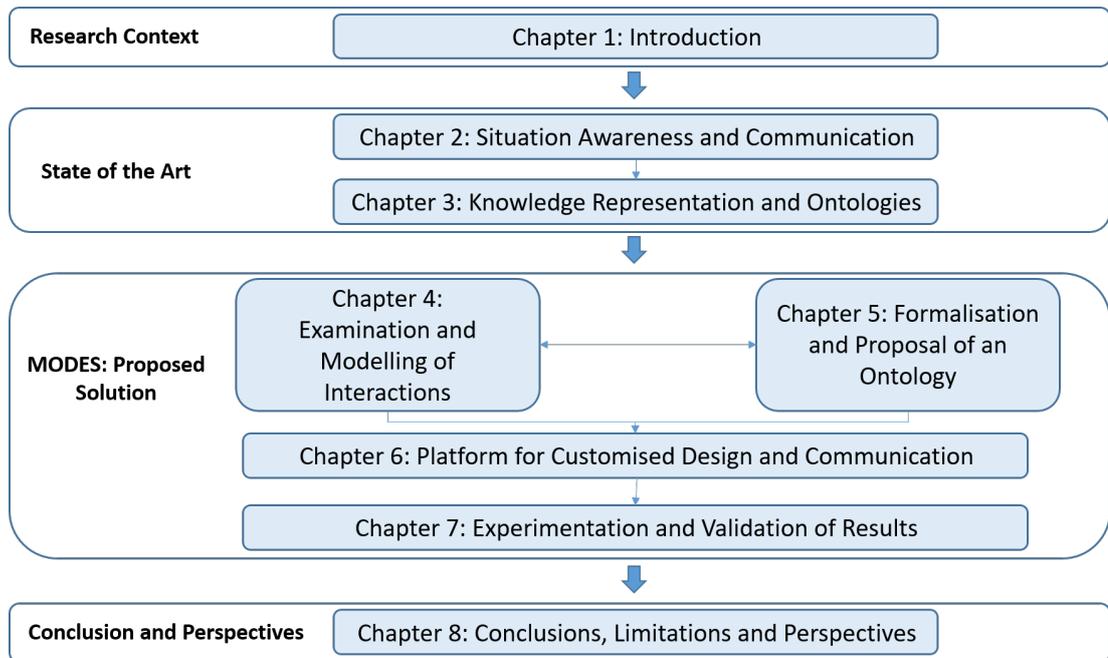


Figure 1.2: Overview of the thesis structure and correlation of chapters.

As we can see in Figure 1.2, the second chapter presents a background on the theory of awareness and the theory of communication. In this chapter, we discuss different types of awareness. We also discuss problems related to awareness and communication in rescue operations. Moreover, this chapter discusses the related work that aimed to support communication and awareness in rescue and emergency response domains. This literature review helped us to identify some research gaps.

1. INTRODUCTION

In the third chapter, we provide further details about knowledge representation. We also give an overview of representation and modelling techniques and discuss the importance of using ontologies for this aim. Details about ontologies, their categories, their languages, and some methodologies of construction are also provided in this chapter. Moreover, several ontology-based systems and existing ontologies related to rescue and emergency domains are presented. Furthermore, several ontology based approaches for designing systems and interfaces as well as ontology-based approaches for access control management are described and analysed with the corresponding ontologies.

In the fourth chapter, we present the different organisations that are involved in French rescue operations, their compositions, as well as the missions of each one. We then present an organisational model that shows the different organisational levels and the hierarchical chain of commands as well as the general flow of information in those operations. Moreover, we provide a scenario of a rescue operation derived from French practices. Afterwards, we identify requirements and parameters to take into consideration for modelling interactions. We then propose a structural model based on those requirements. Furthermore, we propose an interaction model that shows interactions between different actors in the case of French rescue operations.

In the fifth chapter, we propose an application ontology, called ResOnt, to formalise and represent knowledge required to design a communication system oriented for rescue actors that guarantees the confidentiality of information. Therefore, the three modules that form the ontology are presented and described. In addition, a detailed description of the methodology used for creating this ontology as well as a description of the reused ontologies are also provided in this chapter.

In the sixth chapter, we present MODES, a platform that allows users to identify the system's specifications and design its interfaces based on their roles, context, and tasks. The platform's architecture, functionalities, and a use case are presented in this chapter. This platform is based mainly on the interaction model and the proposed ontology presented in chapters 5 and 6 respectively. Thanks to this platform, final users will be able to define the specifications related to information. In addition, each user will be able to design her/his graphical interface in a customised way based on her/his context. On the basis of those specifications and design, end-users will be able to connect to the final system in order

to exchange information. Moreover, the access control policy is presented in this chapter.

In the seventh chapter, we present an overview of different technologies used in the platform implementation. Moreover, we present various functionalities included in the platform. In addition, an example of using the proposed platform is presented. To this end, we describe a communication scenario using the platform in the case of a road accident.

Eventually, in the eighth chapter, we provide concluding remarks and a summary of the main contributions. Moreover, we discuss our work limitations and provide an outlook on future research perspectives.

Publications

Peer-reviewed international journal paper (1)

- **S. Chehade**, N. Matta, J.B. Pothin, R. Cogranne. “Handling Effective Communication to Support Awareness in Rescue Operations.” [Special Issue on “Knowledge, Semantics and AI for Risk and Crisis Management”]. *Journal of Contingencies and Crisis Management*, vol.28, pp. 307-323, September 2020.

Peer-reviewed international conference papers (4)

- **S. Chehade**, N. Matta, J.B. Pothin, R. Cogranne. “Ontology-Based Approach for Designing User Interfaces: Application for Rescue Actors.” *In proceedings of the 17th International Conference On Information Systems for Crisis Response And Management (ISCRAM)*. Virginia, USA, 23-26 May 2020.
- **S. Chehade**, N. Matta, J.B. Pothin, R. Cogranne. “Modelling Interactions in Rescue Operations.” *In proceedings of the 2019 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Bari, Italy, 06-09 October 2019.
- **S. Chehade**, N. Matta, J.B. Pothin, R. Cogranne. “Situation Representation and Awareness for Rescue Operations.” *In proceedings of the 16th International Conference On Information Systems for Crisis Response And Management (ISCRAM)*. València, Spain, 19-22 May 2019.

1. INTRODUCTION

- **S. Chehade**, N. Matta, J.B. Pothin, R. Cogranne. “Data Interpretation Support in Rescue Operations: Application for French Firefighters.” *In proceedings of the 15th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*. Aqaba, Jordan, 28 October to 1 November 2018.

Poster (1)

- **S. Chehade**, N. Matta, J.B. Pothin, R. Cogranne. “Intérêt des technologies mobiles dans le secours à personne.” *Première Biennale de la recherche sur la sécurité civile : L’acceptabilité des risques : Approches pluridisciplinaires*. Aix-En-Provence, France, 06-07 June 2018.

Chapter 2

Communication and Situation Awareness

Contents

2.1	Introduction	18
2.2	Theory of Awareness	18
2.2.1	Definitions and types of awareness	18
2.2.2	Situation awareness	21
2.2.3	Situation awareness in rescue operations	25
2.2.4	Mechanisms for supporting situation awareness	26
2.3	Information Communication	28
2.3.1	Theory of information communication	29
2.3.2	Communication problems in rescue operations	31
2.3.3	Communication and information exchange models for rescue operations and emergency response	35
2.4	Awareness and communication-support systems for rescue and emergency actors	37
2.4.1	Stakeholders' practical needs	38
2.4.2	Criteria and requirements for a usable awareness and communication-support system	40
2.4.3	Analysis of some existing systems for supporting awareness and communication	43
2.5	Conclusions	48

2.1 Introduction

In order to support the concept of awareness in inter-organisational and intra-organisational collaboration, it is necessary to understand and identify its different typologies and characteristics, as well as the different mechanisms required to improve this concept. This chapter of the manuscript aims at presenting the principal areas and concepts addressed in this research that are mainly awareness and communication. We start with the definition of awareness and present its different types. We then focus on a specific type of awareness: Situation awareness, which is the main interest of our work. Hence, we present several models related to this type as well as required mechanisms to awareness. In addition, we examine situation awareness and its importance in our study context that is the domain of rescue. Afterwards, we focus on communication and information exchange as a mandatory step toward reaching awareness. Therefore, we present an overview of the theory of information communication. We then describe problems related to information exchange and communication between different stakeholders in rescue operations. Afterwards, we present some existing works related to enhancing awareness and communications in emergency response and rescue domains. Hence, we examine and discuss several existing models that represent communications and interactions in those operations. Eventually, we present some systems that aimed at supporting awareness in this context as well as the main research gaps drawn from this state of the art.

2.2 Theory of Awareness

Awareness is a multi-faceted term. Several definitions of the awareness concept have been identified in the literature [Bedny & Meister, 1999; Belkadi *et al.*, 2013; Dourish & Bellotti, 1992; Endsley, 1995]. These definitions varies with the variation of the discipline. This section presents the different definitions and types of awareness. Afterwards, the concept of situation awareness which is the main interest of our work is presented in detail. Different mechanisms required in order to support this concept are also presented.

2.2.1 Definitions and types of awareness

It is becoming increasingly evident that awareness is critical to successful collaboration and provides a context for individual activities that facilitate group

progress [Dourish & Bellotti, 1992; Gutwin & Greenberg, 2002]. Awareness was described as perceiving the practices of others, which gives a setting for your own practices [Dourish & Bellotti, 1992]. This context is used to guarantee that singular activities and participation are essential to the group's activity in general and to assess individual actions with respect to group missions and advancement. Moreover, this information enables groups to conduct and maintain collaborative activities [Belkadi *et al.*, 2013].

Awareness has received considerable attention in domains that support cooperative and collaborative environments such as Computer Supported Cooperative Work (CSCW) and groupware research. Such environments are characterised by the implication of one or several teams in order to accomplish a shared goal. Each team is composed of two or more persons that deal with several information resources and work to achieve some common objectives [Stanton *et al.*, 2017]. Distributed teams consist of individuals that interact over space and time through information and information exchange technologies [Fiore *et al.*, 2003]. Several studies have attempted to provide definitions and types of awareness in such environments [Gross *et al.*, 2005; Gutwin & Greenberg, 2002; McDaniel & Brinck, 1997; Salmon *et al.*, 2008]. In this context, researchers and scientists have suggested various types of awareness and have used adjectives to describe the main aspects of this concept. Such types are directly related to different types of requirements concerning awareness. From these types we have:

General awareness: It is defined by Ehrlich & Chang [2006] by the fact of perceiving and understanding the skills of another person and her/his contributions in her/his work. It is represented by the degree of comprehension of the professional experience and skills of this person and how these skills could help you in your work.

Action awareness: It is centred around which actions are being or have been achieved by each actor in addition to the factors influenced or altered by these actions [Carroll *et al.*, 2006].

Activity awareness: It is described as perceiving what is going on around you and involves being aware of the objectives and plans of collaborators [Carroll *et al.*, 2006]. Activity awareness is considered as a specific of awareness and identified as the ability of collaborators to develop and maintain a general picture of effective collaboration [Convertino *et al.*, 2004].

Task awareness: According to [Gutwin & Greenberg, 1995b], task awareness involves understanding the aim of tasks, the specific objectives as well as the requirements of the team carrying in charge of the tasks.

2. COMMUNICATION AND SITUATION AWARENESS

Group awareness: It is defined as the knowledge of the activities of other persons that is required for collaboration and achievement of group tasks. Group awareness is attained by controlling and following information like the locations of other participants in the shared workspace, their tasks and activities, the history of interaction, and their intentions [Gutwin & Greenberg, 1995a]. This awareness term distinguishes multiple types of awareness applicable specifically in collaborative face-to-face activities as shown in Figure 2.1. Figure 2.1 represents the composition of group awareness as defined in [Gutwin & Greenberg, 1995b]. As we can see in Figure 2.1, group awareness includes four types that overlap and are interdependent. These types are social awareness, workspace awareness, group-structural awareness, and informal awareness.

- **Social awareness:** This type focuses on the persons' comprehension of who is around them and with whom they can work and collaborate. It consists of the information that a person maintains about others in a social context such as conversations [Belkadi *et al.*, 2013].
- **Workspace awareness:** This is the most integrated type of awareness in collaboration [Saoutal, 2015]. It involves the collection of up-to-date knowledge that an actor uses to maintain effective interactions with other collaborators within the workplace [Gutwin *et al.*, 1996b].
- **Group-Structural awareness:** This type comprises information about the group itself and its members [Gross *et al.*, 2005]. It consists in the comprehension of the tasks and duties of the members, their work assignments, their rank, and team processes [Gutwin & Greenberg, 1995b].

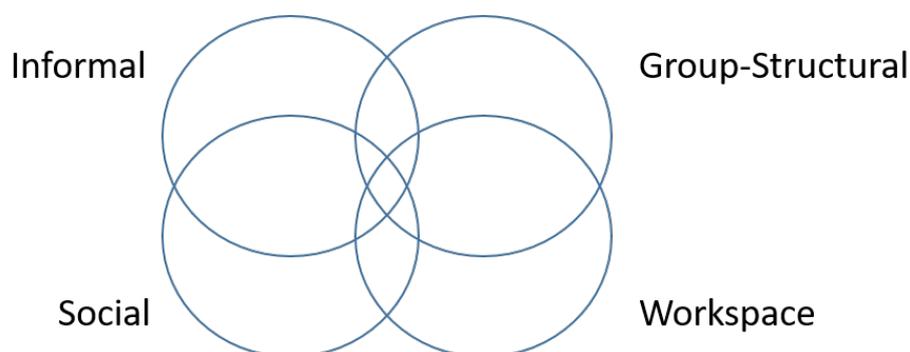


Figure 2.1: Types of awareness in group work.

*Figure adapted from [Gutwin & Greenberg, 1995b].

- ***Informal awareness:*** It consists of general information that collaborators know when they are in the same physical space. Based on this information, they can have a general idea of who is around, what are they doing, and what they are going to do [Belkadi *et al.*, 2013]. Informal awareness is a prerequisite for casual interaction [Gutwin *et al.*, 1996a].

Situation awareness: It is described as the perception and comprehension of a whole situation including situation factors and other collaborators' understandings and plans. This includes responsibilities or modifications of roles; shared plans; task dependencies based on scheduling, roles, and resources [Détienne, 2006]. In our research, we focus on enhancing this type of awareness amongst different stakeholders involved in rescue operations since it is a critical element for decision-making in rescue and emergency response domains. Furthermore, existing related works that aimed at supporting situation awareness are still limited. More details about this concept are given in the following subsection.

2.2.2 Situation awareness

The human factors community has generally discussed the concept of situation awareness. Situation awareness refers to the instant state of knowledge in the world that an individual requires to maintain a complex system or activity. This concept is created through the dynamic process of perception and action and serves as a foundation of overall performance throughout many different domains, such as education, military operations, air traffic control, driving, search and rescue, and crisis management [Endsley, 2006]. More succinctly, it has been recognised as an essential element in decision-making in dynamic and complex situations [Endsley, 1995].

The mostly used definition of situation awareness was given by Endsley [1995] who proposed the cognitive model of situation awareness concerning decision making and performance of actions in complex systems. Endsley defined it as “*the perception of elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future*” [Endsley, 1995]. In addition, she specified required levels toward attaining human situational awareness and divided them as shown in Figure 2.2. Figure 2.2 represents the model of situation awareness and levels toward attaining it as defined by [Endsley, 1995]. As we can see in this figure, those levels are divided into three:

2. COMMUNICATION AND SITUATION AWARENESS

- **Level 1:** The first level of situation awareness is the perception of the situation elements. This requires perceiving all relevant factors that feature a situation together with their status, their attributes, and their dynamics.
- **Level 2:** The second level depends on the first level. It consists in the comprehension of the elements and the current situation. This comprehension depends on understanding the meaning of factors perceived in the first level as well as the relation between these factors and the objectives.
- **Level 3:** The third level involves making predictions about the future status and actions of the situation elements based on the perception and comprehension of these elements during the first two levels. This level cannot be achieved without a sound development of levels 1 and 2 [Endsley, 2016].

Another cognitive model for situation awareness was proposed by Bedny & Meister [1999] who describe situation awareness through an approach based on the

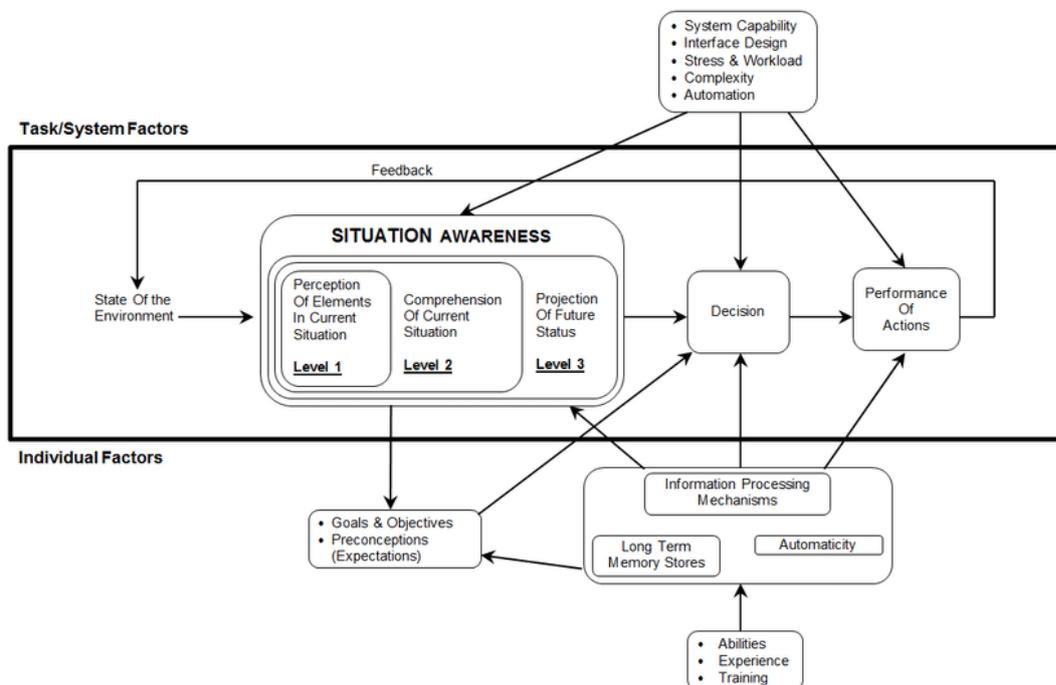


Figure 2.2: Model of situation awareness in dynamic decision making.

*Figure source: [Endsley, 1995].

theory of activity. The latter theory assumes that individuals have objectives that represent a desired final state of activity or an ideal image, motivations that guide them towards the final state and methods of actions that allow the accomplishment of these goals. Differences between the objectives and the actual situation inspire the individual to react toward reaching the objectives. Bedny & Meister [1999] argues that situation awareness can only be understood as a part of intellectual activity and they defined it as *“the conscious dynamic reflection on the situation by an individual. It provides an orientation to the situation, the opportunity to reflect not only on the past, present, and future but the potential features of the situation. The dynamic reflection contains logical-conceptual, imaginative, conscious and unconscious components which enable individuals to develop mental models of external events”* [Bedny & Meister, 1999]. This definition gives a dynamic characterisation to the process of attaining situation awareness. Moreover, the description of how situation awareness alters interaction with the world and how the world alters situation awareness is coherent and goes beyond the description provided by Endsley [Endsley, 1995; Salmon *et al.*, 2008]. Figure 2.3 shows the interactive sub-system approach to situation awareness proposed by Bedny & Meister [1999]. Each block presented in Figure 2.3 orientates itself toward the development of awareness and has a special role in the achievement and maintenance of situation awareness. As we can see in Figure 2.3, the individual’s goals and objectives presented in block 2, their experience presented in block 7, and the conceptual model of the actual situation in block 8 affect the way of interpretation of incoming information in block 1. This interpretation then influences an individual’s objectives and experience as well as the conceptual model of the actual situation. Afterwards, important contextual features are determined based on their importance to the task objectives and motivations toward them, which guides their interaction with the world. Blocks 4 and 5 in Figure 2.3 represent these two functions respectively. The degree to which the individual continues to draw in the task objectives is dictated by their objectives represented in block 2 and their assessment of the actual situation presented in block 6. The resultant experience of an individual derived from her/his interaction with the world is gathered as experience that illuminates the conceptual model in block 8. According to the model, the fundamental processes involved in the development of situation awareness are the image goal, the conceptual model, and the relevant task conditions.

From the above definitions, situation awareness can be expressed as the outcome

2. COMMUNICATION AND SITUATION AWARENESS

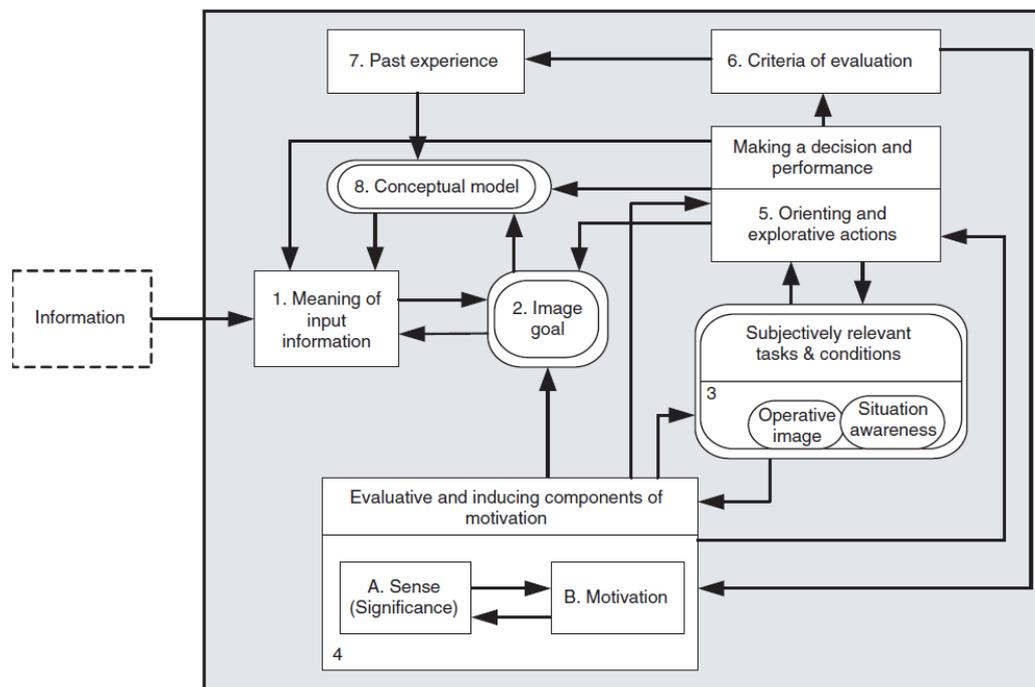


Figure 2.3: Interactive sub-systems approach to situation awareness.

*Adapted from [Bedny & Meister, 1999].

of knowing what is going on around and serves as the foundation for decision-making [Artman & Garbis, 1998]. Researchers in different areas have determined that expert decision-makers start with classifying and understanding a situation, and proceed then to decision making [Endsley, 1995; Kulyk *et al.*, 2008]. However, regardless of the adopted definition, the ability to acquire situation awareness as well as the ability of understanding and projection is not necessarily identical for different people who have perceived the same information. This ability depends on the individual information processing mechanism which is related to the personal capacity, experiences, and training. This means that even if the situation awareness is related to decision-making and task performance, it is explicitly recognised as a concept separate from these two concepts. Endsley [1995] points out that the best decision-makers may make the wrong decisions because of inaccurate or incomplete situation awareness and that, oppositely, a person who is perfectly aware of a situation can still make the wrong decision due to a lack of experience or an inability to carry out the necessary actions.

2.2.3 Situation awareness in rescue operations

Situation awareness has vital importance in collaborative environments since it can improve team performance by improving the quality of made decisions [Endsley, 1995]. In rescue operations, establishing a high level of situation awareness is fundamental to lessen undesirable consequences. This awareness may help to anticipate unexpected scenarios and prepare adequate plans. In numerous rescue operations and emergency response training programs, students are shown the benefits of visualising the situation before arriving at the intervention site. This visualisation helps to perform primary analysis of the situation and to decrease the response time. Intervention team members usually have a certain period while heading toward the intervention site. During this time, it is very interesting to analyse and examine the available information such as the description of the accident and to predict what kind of difficulties can be encountered by the intervention team in the near future [Shimanski, 2008]. For instance, a rescuer may realise that rescuing a harmed climber on the other side of a valley means that the intervention team will need to implement a specific framework to cross over a large river. Therefore, team members will be able to anticipate and prepare the plans required to create the Tyrolean system necessary for crossing the river [Shimanski, 2008]. Similarly, the intervention team members can discuss their pending rescue while heading toward the intervention site. For example, during a recent rescue operation following an avalanche, rescue team members were playing out a specialised lowering of the victim to a relevant expanse where the helicopter could load the victim. During that lowering, team members were staying in their helicopter at the parking lot and discussing in detail the ways to react and evacuate the victim. They could have been talking about their personal life or other subjects, however, they took benefit of the opportunity to brief each other on the distribution of tasks and missions and on what potential difficulties would happen [Shimanski, 2008]. Effects of situation awareness go beyond the anticipation of operations and its importance is not limited to this aspect. Situation awareness is a crucial characteristic required when different services and actors involved in rescue operations must collaborate to cope with a significant incident that may trigger life-threatening effects. If the involved actors and services focus only on their activities, this is a consideration that creates information-gaps [Norri-Sederholm *et al.*, 2017]. These actors ought to recognise each other's main elements, such as goals, skills, requirements, aspirations, procedures, experiences, and procedures, in order to ensure successful collaboration.

2. COMMUNICATION AND SITUATION AWARENESS

Unfortunately, reaching a high level of situation awareness is one of the most problematic duties in many activities and one of the most challenging tasks for rescue actors [Endsley, 2006]. Rescue operations are characterised by the multiplicity of intervening organisations, having different cultures and objectives. A direct result of this multiplicity is the constraint that the actors are not all aware of the objectives and priorities of others, which means that actors are not aware of what is relevant to other actors. Ensuring a high level of awareness requires managing and achieving diverse activities and mechanisms such as effective communication, interaction, and information exchange. These activities and requirements are presented in the following subsection.

2.2.4 Mechanisms for supporting situation awareness

Understanding the manners and mechanisms required for maintaining awareness is critical as a primary step toward designing systems that aim at supporting it. Maintaining awareness has proved to be challenging in real-time distributed environments where communication services are limited and interaction processes are complicated. As a consequence, working together through a groupware system often seems complex and inefficient compared to working in the same physical place that enables the visualisation of other collaborators' activities. It is becoming increasingly clear that being aware of others' activities and situations plays an significant role in the naturalness and flexibility of collaboration. Furthermore, supporting the awareness toward other collaborators is seen as one way to minimise the peculiarity and difficulty of remote cooperation and collaboration [Gutwin & Greenberg, 2002]. According to Gutwin & Greenberg [2002], this difficulty results from groupware technologies that limit the ability of persons to perceive information about the activities of others in the workspace, which hinders their ability to collect information related to workspace awareness from the environment. Gutwin & Greenberg [2002] proposed to support workspace awareness. To this end, they proposed three required mechanisms for this aim. The first mechanism is consequential communication that consists in watching other people's actions which allows a visual perception of others' elements and activities. The second mechanism is artefacts that represent the second source of awareness information [Dix *et al.*, 2003]. An artefact serves in enhancing awareness by providing relevant information when an artefact is manipulated or affording multiple functionalities that facilitate the comprehension of situations. Whereas, the second mechanism is intentional communication which forms the

third source of information through gestures and conversations in a group [Clark & Brennan, 1991]. Verbal communications are the dominant mode of interactions in most groups, and three ways allow obtaining information awareness through verbal conversations. First, individuals may explicitly discuss with their collaborators regarding the aspects of awareness. For instance, they clearly state where they are operating and what are their activities. Second, individuals can collect information related to awareness by hearing the conversations of others even if these individuals are not directly involved in the discussions. While the third way is when individuals observe and analyse the commentary that collaborators produce together with their actions [Gutwin & Greenberg, 2002]. Another mechanism to support awareness was proposed by [Schmidt, 2002] who emphasises that awareness is not a product of passively captured information, but it is a characterisation of certain very active and highly qualified practices. The aforementioned mechanism consists in displaying and monitoring activities. Thanks to this approach, collaborators can track the activities of their colleagues by visualising or listening in order to determine the progress, state, and evolution of these activities and thus to determine whether they are being executed as expected or there is a need to make some adjustments [Schmidt, 2002].

Another way to collect the elements of awareness is through the use of the context. Kirsch-Pinheiro *et al.* [2004] emphasises that the concept of awareness must use the notion of context to adapt the content provided to the user. Context is defined by any information that can be used to describe an entity's condition. An entity can be an object, place, or person that is perceived to be important to the relationship between the user and the system, including the user and the systems themselves [Abowd *et al.*, 1999]. Kirsch-Pinheiro *et al.* [2004] used the notion of context to adapt the information provided to the user and proposed representation of the context for an adapted awareness mechanism. This approach allows to filter the information provided to users according to the description of the group context, role definition, activity, and the work process.

[Javed *et al.*, 2011] proposed another mechanism that aims at supporting communications and shared situation awareness, which was defined as “*the degree to which each team member has the same situation awareness or understanding of a situation*” [Endsley & Robertson, 1996]. This mechanism is based on the use of an ontology-based and semantic technologies approach which helps to unify the understanding of the situations between different stakeholders and thus to unify operational pictures and situations' perceptions between them. Ontology is generally interpreted at two levels. First, it serves as a knowledge base for a given

2. COMMUNICATION AND SITUATION AWARENESS

domain. In addition, at a second level, it provides a vocabulary that uses relevant concepts to identify domain or situation elements or factors and protocols for connections and communications between them. Thus, ontologies offers a common interpretation of messages that can be expressed by users which enhances shared situation awareness [Javed *et al.*, 2011]. Endsley [1995] also recommended mechanisms to improve situation awareness. These mechanisms consist of presenting the information in a simple way that facilitates the understanding and prediction levels in situation awareness that correspond to levels 2 and 3 respectively in his proposed model. Endsley [1995] also suggested organising information in a way that is compatible with the objectives of the people as well as highlighting important clues to grab attention during critical events.

In our research, we focus on improving the concept of awareness in a complex, dynamic, and distributed context that involves a collaboration of the different actors brought to carry out their interdependent activities. To this end, we put the link between the situation awareness and ensuring a common perception of situations through guaranteeing effective information exchange in an inter-organisational collaboration in dynamic situations. It is about the timely perception of the right information related to interdependent activities in order to integrate and complete these activities. This requires systems to help the different actors to easily perceive this information according to their context in order to improve their awareness and lead them to carry out their activities. The question we are currently asking is how to facilitate actors collecting good information on situations and what is happening around them in order to make the right decisions and carry out adequate actions. For this aim, we study mechanisms required for handling effective information exchange in order to enhance situation awareness in rescue operations.

2.3 Information Communication

Handling effective communications is mandatory in rescue operations since it is the only way to establish a common representation of situations between actors through exchanging information about situations, dangers, casualties, resources, and locations of intervention teams. By sharing these and other information, a common background about the on-going operation can be shared by different actors, which essentially consists of the two first steps toward reaching situation

awareness. In this section, we present principles of communication and information exchange through an overview of information theory. Afterwards, we discuss the main problems related to communication between different stakeholders in rescue operations. Several solutions that aimed at supporting awareness and communications in rescue operations are then presented together with the limitations of each one.

2.3.1 Theory of information communication

Communication is a phenomenon to request and send knowledge and information. It is defined as a dynamic process of generating, receiving, and understanding messages that produce a response [Griffin, 2006]. It represents a phenomenon that involves reading and writing, listening and talking, observing and performing, or doing anything that requires messages in any medium or circumstance [Craig, 2006]. It can be in several forms such as ordinary conversation, interpersonal communication, online communication, phone communication, written communication, and mass media [Atifi, 2016]. The general system of communication and information exchange was elaborated in 1949 by Shannon and Weaver, two theorists of communication, who proposed a mathematical theory of communication [Shannon & Weaver, 1949]. The proposed model serves till these days as a basic model for communication. Influenced by the signal transmission systems, this model described communication as the propagation of a message from a source to a destination in the form of a signal and implied that communication takes place only in one direction at a certain time. The transmitter encodes a message and uses a certain channel to send it to a receiver that decodes and interprets it [Atifi, 2016]. Figure 2.4 shows the general model of communication proposed in [Shannon & Weaver, 1949]. As we can see in Figure 2.4, the proposed model

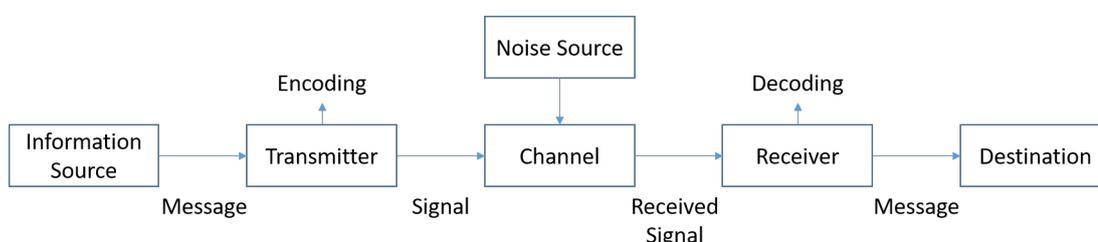


Figure 2.4: General communication model.

*Adapted from [Shannon & Weaver, 1949].

2. COMMUNICATION AND SITUATION AWARENESS

consists of seven components. The first component is the information source that selects a desired message, which is the second component and may consist of pictures, videos, or spoken words. This message is encoded by the transmitter that represents the third component and transforms the message into a fourth component: the signal. Hence, this signal will be transmitted from the transmitter to the receiver through the communication channel that constitutes the fifth component and is affected by noise sources. Once delivered, the transmitted signal is decoded by a sixth component: the receiver that reconstitutes the message and transmits to the seventh component: the destination.

Another alternative view to communication was proposed in Wiener [1949] who considered that communication is not limited to the transmission of information in unidirectional mode. However, communication includes the major dimension of reciprocal interaction. In this process, the message receiver reacts and formulates a response message and addresses it to the original transmitter, which becomes a receiver in its role, and so on [Wiener, 1949].

Several studies were conducted to study, analyse, and enhance communications. For example, Shannon and Weaver studied ways to increase the efficiency and accuracy of transmission and reception. They focused on the exchange of information by studying the messages, channels, encoding, and decoding methods rather than the meaning of messages. Other researchers studied communication as a phenomenon that has three approaches: syntax, semantics, and pragmatics [Watzlawick *et al.*, 1972]. The first approach concerns the transmission of information. It deals with several aspects such as transmission channels, coding problems, noise capacity, and redundancy. The semantic approach centred on how the meaning of the message is created and understood. The interpretation of the messages relies on how we understand the terminology used by the sender. In order to be successful, any information exchange presupposes a semantic convention between the holding parts. Hence, an agreement on the meaning of messages should take place between the sender and the receiver. Whereas pragmatics deals with words and their meanings and emphasises non-verbal communication [Watzlawick *et al.*, 1972].

Effective communication depends on how people perceive each other's intentions and how they interpret messages [Salo-Lee, 2006]. Schmitz *et al.* [2012] defined perception as the process of selection, organisation, and interpretation of information. Information selection is a processing convolution in which people focus their attention on certain incoming sensory information. The organisation of information consists in sorting and classifying the information that we perceive

according to the innate and learned cognitive schemes. This organisation is done using three strategies: proximity, similarity, and difference [Saoutal, 2015]. While the interpretation was defined by Schmitz *et al.* [2012] as a process of assigning meaning to the information using mental structures or diagrams. For this, interpretation is affected by the context as well as all the aspects linked to a situation. Tools used to access and transmit information plays a key role in communication and specifically in distance communication. People always encounter have difficulty in case of remote communication. This is due to the difficulty of locating relevant sources of information, the difficulty of physical access to sources, the cost in time and effort as well as problems credibility and reliability of the sources [Olivesi, 2014]. Information and communication technologies aim to remedy these problems and facilitate remote communication through communication tools. However, these tools may not be effective if they do not allow the perception of information. People in a collaborative context need to perceive information in order to carry out their activities. This perception is part of the process of achieving awareness which is considered to be an important aspect in socio-technical perspectives and plays a key role in decision-making, the coordination of activities, and their performance [Smith & Hayne, 1991].

2.3.2 Communication problems in rescue operations

Handling effective communication in rescue operations remains a challenging problem. The essence of this challenge is to be mindful of the information needs of the other collaborating actors, to efficiently exchange accurate and timely information with the correct recipients, and to recognise what information is probably to be demanded [Munkvold *et al.*, 2019]. Several recent studies reveal persistent communication problems between different stakeholders in rescue and emergency response domains [Bunker *et al.*, 2015; Steen-Tveit & Radianti, 2019; Steigenberger, 2016; Wolbers & Boersma, 2013]. This is due to many reasons. First of all, the most common difficulty is the highly dynamic aspect of contexts and situations. Consequently, continuous communication has to be maintained, which entails a large amount of information to be transmitted, derived, and processed. Second, effective communication requires a common interpretation of the information by different entities. In rescuing, it is difficult to meet this requirement since each operation requires the engagement of multiple actors. Everyone involved has her/his professional background and experience level. Finally, information exchanged during those operations can take different forms and categories. For

2. COMMUNICATION AND SITUATION AWARENESS

example, it can be in the form of texts, photos, audio, videos, or signals and it can be organisational, situational, spatial, and medical. Table 2.1 shows different groups of information and information elements that actors are supposed to exchange and visualise during a rescue operation. These groups and elements were identified based on a study of domain related documentation such as reports as well as previous studies in the literature review [Li *et al.*, 2014; Yang *et al.*, 2009; Zhang *et al.*, 2011].

Table 2.1: Main groups of information and information elements required by participating actors in rescue operations.

Group of information	Information elements	Category
Incident information	Incident, Address, Date and Time	Situational
Intervention site accessibility and general information	Type, Function, Address, Road to take, Time to arrive, Distance	Spatial, Situational
General information about victims	Name, Sex, Age, Age Range, Gravity, Status, Localisation	Medical
Specific dangers	Danger, Localisation	Situational
Centres' cartography	Name, Address, Accessibility	Spatial
Material cartography	ID, Material, Number, Availability, Localisation	Organisational
Persons' cartography	ID, Name, Availability, Skills, Role, Function, Affiliation, Localisation	Organisational
Material to engage	ID, Material	Organisational
Actor to involve	ID, Name, Skills, Role, Function, Affiliation	Organisational
Encountered problems	Problem	Situational
Engaged material	ID, Material, Number, Status	Organisational

2.3 Information Communication

Involved actor	ID, Name, Skills, Role, Organisational Function, Affiliation	
Departure and arrival information	Date, Time	Situational
Resources	Capacity, Localisation	Organisational, Spatial
Environmental conditions	Fire surface, Surface contaminated, Air humidity, Wind speed, Air temperature	Situational
History of the intervention	Initial situation, Final situation	Situational
Requests for material	Material, Number	Organisational
Requests for actors	Role, Function, Skills, Affiliation	Organisational
Evolution of the situation	Occurrence of events	Situational
Intervention teams information	Localisation	Spatial
Achieved and current tasks	Task, Time, Name of responsible, ID of responsible	Situational
Medical record	ID, Name, Sex, Age, Age Range, Gravity, Status, Localisation, Vital parameters, Occurrence of medical events, Achieved Gestures, Oxygen Saturation, Blood Pressure, Body Temperature, Tension	Medical
Medical history of victims	Antecedents	Medical
Hospitalisation centres accessibility and availability information	Name, Address, Availability, Distance	Spatial
Decisions information	Decision, Role of responsible, Function of responsible, Skills of responsible	Situational

2. COMMUNICATION AND SITUATION AWARENESS

As we can see in Table 2.1, groups of information that actors are supposed to communicate and visualise in rescue operations are heterogeneous in terms of elements and categories. This heterogeneity makes the activity of actors difficult. Figure 2.5 shows the multiplicity of involved actors and information flow between them. As we can see in Figure 2.5, different multiple actors participate in a single rescue operation. They execute their tasks, communicate, and exchange an enormous volume of information like medical and situational information. This plurality of sources and the important volume of exchanged information during an operation can lead to overcharge and make it challenging for actors to understand the provider's intentions. All the aforementioned difficulties in communications and information exchange between different stakeholders in rescue operations lead us to choose supporting interactions and communications in order to enhance situation awareness in these operations.

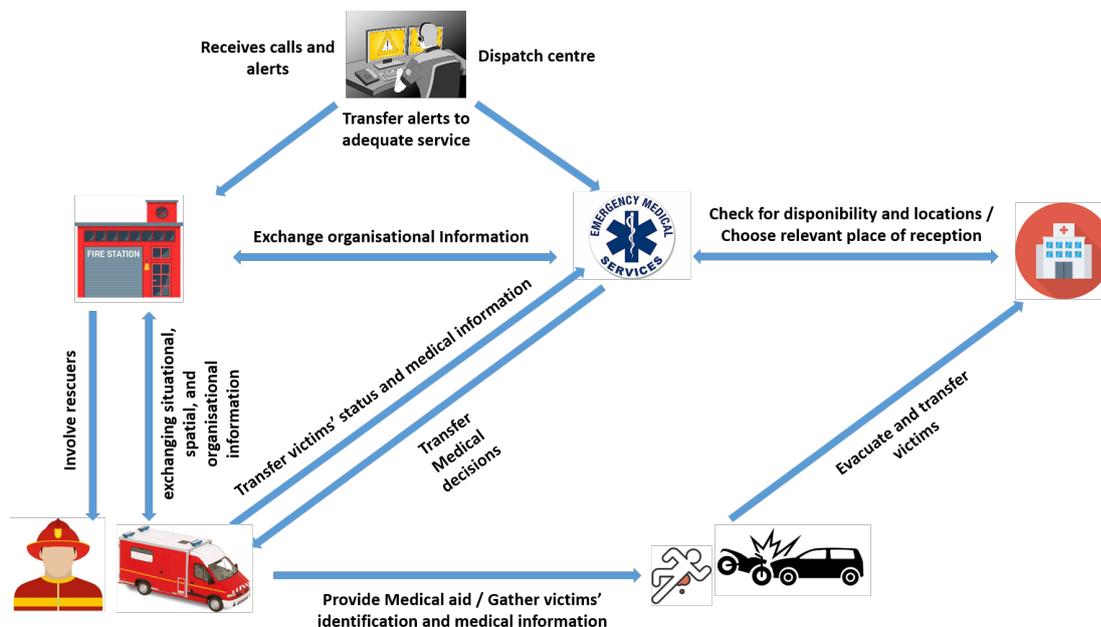


Figure 2.5: Information flow and complexity in rescue operations.

2.3.3 Communication and information exchange models for rescue operations and emergency response

The improvement of communication and information sharing in rescue operations has been the topic of numerous studies over the past decades. Numerous solutions have been developed attempting to solve serious problems that lead to inefficient decision-making such as lack of situation awareness and inefficiency in information sharing. In this context, several systems were developed to support information exchange and communication. Some of those systems are presented in the next section. Moreover, several studies have been carried out to improve situation awareness in rescue operations. Some researchers worked on identifying information needs as a first step toward supporting communication and awareness. For instance, a study was conducted in [Yang *et al.*, 2009] to identify information requirements for emergency response according to actors' roles. Unfortunately, identified requirements were limited to those related to on-site responders without considering other actors' needs. A similar study was conducted by Li *et al.* [2014] to improve situation awareness amongst actors involved in emergency response operations. To this end, authors have evaluated the information needs by first responders to develop and maintain on-scene situation awareness. Sources for obtaining the required information and implementation requirements for situation awareness were also identified. Surprisingly, a specific kind of emergency was taken into consideration in the study that is building fire without considering other types of emergencies.

On the other hand, research on modelling processes, communications, and interactions in emergency response and rescuing has evolved lately. Several process, communication, and interaction models are proposed in the literature as shown in Table 2.2. Table 2.2 shows four selected models that were created to analyse and formalise knowledge related to processes and interactions in rescue operations, emergency response, and crisis management. As we can see in Table 2.2, some researchers used methodologies based on business process modelling techniques and diagrams. Saoutal *et al.* [2014] conducted a study to determine problems related to information exchange in inter-organisational emergency response and crisis management. They also modelled communication between different stakeholders by using UML diagrams. The proposed model included dependencies between actions, actors, and information but it does not take into consideration the information support, which is an essential element for communication.

2. COMMUNICATION AND SITUATION AWARENESS

Table 2.2: Communication and interaction models for rescue operations and emergency response.

Model	Principle	Contribution	Limitations	Reference
Communication model for crisis management	Modelling the communications using UML diagrams	Actors' interactions; Dependencies between actions, actors, and information	The sources and destinations of information are not shown	[Saoutal <i>et al.</i> , 2014]
Coordination process model	Modelling coordination using Business Process Modelling Notation	Interactions and coordination process in crisis management	The information exchanged at each step of the response is not shown	[Truptil <i>et al.</i> , 2010]
Fire emergency response process model	Modelling processes and interactions using Business Process Modelling Notation	Processes and interactions in fire emergency response	The requirements in terms of information are not considered	[Nunavath & Prinz, 2015]
Environmental, Role and Interaction model for crisis management	Proposing a multi-agent organisational model using the GAIA methodology	Environments, roles and interactions in crisis management	The information flow is not shown in the interaction model	[Chaawa <i>et al.</i> , 2017]

Another limitation of the proposed model is that it does not show the destinations and sources of information. In the same context, authors in [Truptil *et al.*, 2010] proposed to support coordination in crisis response through the IsyCri project by providing a mediation information system. To do that, they proposed a coordination process model that shows different interactions between actors using Business Process Model Notation. However, the proposed model does not show what is the exchanged information between those actors at each step of the response. Similarly, Nunavath & Prinz [2015] choose to model the emergency

2.4 Awareness and communication-support systems for rescue and emergency actors

management process in Norway by using Business Process Modelling Notation. This work aimed at supporting coordination and information sharing between different stakeholders involved in emergency response. To this end, an emergency management model was proposed showing the sequence of different tasks together with the responsible stakeholder. Unfortunately, the requirements for each participating actor in terms of information were not taken into consideration in the aforementioned model. Hence, the proposed model cannot serve as a basis for analysing and formalising interactions between different actors. Other studies were based on methodologies oriented for agent architectures. A recent study was conducted by Chaawa *et al.* [2017] to model crisis management procedures and interactions between different actors in order to propose a flexible and usable crisis management system. To this end, three different models were proposed based on the GAIA methodology oriented for multi-agent architectures [Wooldridge *et al.*, 2000]. The first model is an environmental model that identifies different concepts related to crisis management such as infrastructures and resources together with the information related to each concept. The second model is a role model that includes different tasks with the associated responsible actor. This model also highlights the various tasks that require interactions between different actors. While the third model is an interaction model that illustrates communications between different actors. Unfortunately, the information flow between different actors is not shown in the interaction model. Moreover, the role model does not illustrate the sequence of different tasks. In addition, dependencies between tasks and information and those between the roles of actors and information are not shown in any of these models. Therefore, the use of these models is limited and requires further analysis.

2.4 Awareness and communication-support systems for rescue and emergency actors

Several systems were developed to support awareness, information exchange, and communication in rescue operations. However, their use is still limited [Mallek *et al.*, 2016]. In our opinion, the main reason behind this problematic is that the majority of these systems does not meet the criteria that a usable communication and awareness-support system oriented for rescue actors has to fulfil. Moreover, in our best knowledge, only few of those systems responds to the diversity of stakeholders' needs. In this section, we first list the main stakeholders'

2. COMMUNICATION AND SITUATION AWARENESS

needs related to a communication system that supports their practices. We then list the central criteria that an efficient and usable awareness and confidential communication-support system has to fulfil in order to be useful in rescue operations. The importance of this step is that it serves as a basis in order to define specifications, architecture, and functionalities of the system to design. We then present some existing communication systems oriented for rescue services and actors and we analyse how each system responds or not to the identified needs and criteria.

2.4.1 Stakeholders' practical needs

In order to achieve successful operations, different involved stakeholders' share a common requirement: being able to communicate efficiently and reaching a high level of situation awareness. Achieving efficient communications and awareness has led to the identification of several stakeholders' needs. Those needs are defined based on the definitions of situation awareness, domain related documentation, problems pointed out by the stakeholders', as well as several previous studies. The principal needs are identified as follows:

- ***Common Terminology:*** A first key for ensuring a common situational understanding is ensuring a common interpretation of information between different actors. Therefore, a unique terminology must be in use by different actors in order to ensure the common interpretation of information. Hence, the system must be designed in a way to obtain a common terminology that can be accessible by different stakeholders. Essential techniques that can be used in this context are the semantic representation of data and ontologies that can be very helpful in order to ensure common situations' representations and data interpretation between actors [Nunavath *et al.*, 2013].
- ***Interoperable communications between all the services:*** Rescue operations require the involvement of multiple actors from different services. Hence, it is mandatory to allow different actors from various services to communicate with other actors in order to maintain the required collaboration. Therefore, regardless of their roles, all actors involved in rescue operations must be able to exchange and visualise information. For instance, the operators and decision-makers in command centres must be allowed to receive

2.4 Awareness and communication-support systems for rescue and emergency actors

and visualise situational information from intervention teams to take relevant decisions. Similarly, intervention teams' members should be able to transmit organisational, situational, spatial, and medical information and receive decisions from command centres and hospitalisation centres. Moreover, despite their affiliation, stakeholders' should be able to communicate efficiently with each others without any barrier. Hence, the requirement for interoperability between different services is one of the principal stakeholders' needs [La DDSC et la DHOS, 2009].

- ***Exchange of different required types and forms of information:*** Rescue actors require access and support for any type of communication through the required communication device. For instance, intervention teams need to use mobile phones in order to exchange information with rescue centres. Whereas, operators in rescue centres should be able to handle non-oral communications through desktops. Furthermore, rescue operations require the communication of different information groups and elements such as organisational information on resources and cartography, as well as medical information like the number and seriousness of victims along with their records. Those groups and elements are presented in Table 2.1. Hence, it is fundamental to allow the communication of different types of data. In order to facilitate the stakeholders' tasks, the different pieces of information identified previously can be exchanged in various forms, which leads to other essential requirements. For example, rescuers might share photos or videos from the scenes to share a clear operational picture. Moreover, they may send voice messages to simplify their tasks by avoiding typing. Thus, actors should have the ability to exchange different forms of data during the operations.
- ***Resources Allocation:*** The resources allocation consists in determining the required medical and operational resources required according to the incident and to the victims' status. It also consists in involving and engaging the selected resources. In rescue operations, due to the enormous amount of generated information and the rapid evolution of events, different services may be upset and irrelevant decisions may be made. Consequently, resources are managed improperly, which may affect the victims' lives [Elmhahbi, 2020]. Therefore, rescue actors should needs a support for resources allocation through a decision-support system. For instance, reg-

2. COMMUNICATION AND SITUATION AWARENESS

ulator doctors should be supported during the choice of the hospitalisation centre of reception.

- ***Exchange of actionable information based on contexts:*** Rescue actors have different missions that vary according to their affiliations, roles, and contexts. Those rescue actors handle different tasks that are defined based on their roles and skills. They are supposed to support, consult or transmit information based on the task being handled. This causes a heterogeneity in the actionable information required by each person based on the context, role, and time. In other words, people in different roles may want different information in different forms at different times [Zade *et al.*, 2018]. Accordingly, rescue actors need to exchange the right information to the right person at the right time. This will improve the utility of exchanged information and solves the problems related to information overload.

2.4.2 Criteria and requirements for a usable awareness and communication-support system

Any usable system that aims at enhancing situation awareness and ensuring effective communications in rescue operations must meet a list of minimum criteria. Those criteria are defined based on the definitions of situation awareness, domain related documentation, stakeholders' needs, as well as several previous studies. They include ensuring taking into consideration the diversity of stakeholders' needs, personalisation and adaptability to users' contexts, flexibility, and eventually, guaranteeing confidential access to information.

- ***Taking into account the diversity of stakeholders' needs:*** Multiple stakeholders from distinct organisations and services participate in a rescue operation. Those stakeholders have different needs and requirements according to their roles, missions, and contexts. Therefore, it is very important that the system can respond to the stakeholders' needs regardless of their roles and contexts. The principal stakeholders' needs identified in this work are presented in section 2.4.1. They include: Common terminology, Interoperable communications between all the services, Exchange of different types and forms of information, and Resources allocation.

2.4 Awareness and communication-support systems for rescue and emergency actors

- ***Personalisation and adaptability to users' contexts:*** Rescue operations and emergency response are complex domains that present specific requirements for involved actors. Those actors have to make decisions and operation within short periods of time with often missing information or overload of data through which it is challenging to retrieve relevant information [Carver & Turoff, 2007]. To this end, they must be able to absorb information rapidly, understand its meaning and relevance, and decide what are the relevant actions based on this information. Moreover, rescue operations and emergency response are exceptional events characterised by stress especially in case of reduced comprehension of reality or loss of control over the situation where additional stress is caused [Döweling *et al.*, 2009]. Therefore, it is very important that supporting systems help to reduce the actors' cognitive load. Hence, the system should be personalised according to the users' preferences. Moreover, participating actors have different missions that vary according to their affiliations and roles. They always come from distinct backgrounds with various levels of experience. Furthermore, rescue actors handle different tasks that are defined based on their roles and skills. They are supposed to support, consult or transmit information based on the task being handled. This causes a heterogeneity in the information to exchange and visualise depending on the context and role of each actor. Accordingly, the system should be adaptable to the context of its users in order to prevent information overload. Several researchers have begun to argue for the need to shift from a focus on supporting a common operating picture to developing mission-specific tools [Zade *et al.*, 2018]. Therefore, the system must take into account the preferences of various actors. In addition, it must be adaptable to users' contexts. According to [Coche *et al.*, 2019], the use of meta-models and ontologies can be very helpful for this aim.
- ***Flexibility:*** A high level of and flexibility is required in the domains of rescue and emergency response. This is due to the continuous and unavoidable evolutions in the processes and organisations in these domains [Bénaben *et al.*, 2008]. Unfortunately, in most of the countries, rescue operations and emergency response are organised in different ways in compliance with local laws, regulations, and practices. Hence, the majority of systems oriented for rescue and emergency response actors are designed specifically for each country, or even for a particular region or hospital. Such systems have two

2. COMMUNICATION AND SITUATION AWARENESS

main inconveniences. The first one is represented by a lack of generality and flexibility due to their reliance on non-standard rescue and emergency response models. This hinders their effectiveness and restricts their re-usability and applicability to other emergency contexts or to modifications on the rescue and emergency response regulations and workflows. Second, in case of need, the design and development of new systems consumes a lot of resources compared to slight modifications in existing systems [Valls *et al.*, 2010]. Therefore, communication and awareness-support systems designed to sustain emergency response and rescue operations are very demanding in terms of ensuring flexibility and adaptability to the requirements of the domain and its long-term transformation and growth. This transformation can occur due to many reasons such as the integration of new technology solutions, modifications in domain concepts and procedures or the addition of new ones. The real question is how to include adaptability and flexibility in the systems design method. Essential techniques that can be used in this context are the semantic representation techniques and ontologies that can bring several benefits with regards to adaptability, flexibility, and work efficiency from the end-user point of view [Bénaben *et al.*, 2008; Valls *et al.*, 2010]. According to Valls *et al.* [2010], ontologies promote the adaptation to shifts in highly dynamic domains such as the domain of healthcare or rescue. Furthermore, ontologies support the creation of profile and role-based interaction models and enhances the generality and re-usability of the designed systems.

- **Confidentiality:** Since rescue operations require the communication of personal and medical information, it is fundamental to ensure the confidentiality of those communications. In other words, it is mandatory to guarantee the privacy, reliability, and integrity of exchanged information. For that reason, the communication system must guarantee this confidentiality by integrating several techniques such as the anonymisation and encryption of data, data versioning, as well as users' authentication to prevent forbidden access [Channa & Ahmed, 2010]. Furthermore, participating actors have different roles with distinct grades and functions. These differences in roles result in differences in communication needs and permissions. For example, an operator is not allowed to access medical information of victims while a regulator does not need to obtain organisational information such

2.4 Awareness and communication-support systems for rescue and emergency actors

as information about resources. It is therefore necessary to restrict communications and system functionalities according to actors' roles and grades. Moreover, each rescue operation is handled by one or several intervention teams that are composed of specific members. Hence, access to information related to each operation should be restricted to the members of teams that participate in the intervention. In this manner, it is essential beyond the communication features to consider the information system access control.

2.4.3 Analysis of some existing systems for supporting awareness and communication

Numerous solutions have been developed attempting to solve serious problems that lead to inefficient decision-making such as lack of situation awareness and inefficiency in information sharing. In this context, several systems were developed to support information exchange and communication. Some of these systems were oriented for medical information exchange, others are specified for organisational, spatial, and situational information communication, while some systems were developed to support the communication of medical, organisational, spatial and situational information in rescue and emergency response operations.

2.4.3.1 Organisational, spatial, and situational information exchange systems

Meissner *et al.* [2006] proposed MIKoBOS a system that aims at ensuring a reliable data exchange within and between different involved organisations during emergency responses. MIKoBOS aimed at enabling rescue teams to share organisational and operational information such as situation reports and available resources. The proposed easy to use and personalised system helps to ensure a common operational picture between different actors, takes multiple actors' roles into consideration, and consists of three application components: MIKoBOS-EP for front-line responders at the intervention sites, MIKoBOS-TEL for on-site operation commanders and MIKoBOS-LS for headquarters. Furthermore, thanks to MIKoBOS, rescue actors are allowed to exchange different forms of organisational and situational information such as texts, pictures, sensor data, and videos. In addition, the system is designed in a way that makes it flexible and adaptable for different contexts. For instance, it is possible to adapt the data stream to available communication conditions according to associated policies. Unfortunately,

2. COMMUNICATION AND SITUATION AWARENESS

mechanisms related to information confidentiality were not integrated into the proposed system. Another communication support system oriented for emergency response was proposed in [Monares *et al.*, 2011a,b]. This latter consists of a mobile application called MobileMap that is oriented for teams at intervention sites. It also includes a decision support module called DDSS that is used in operational and command centres. Intervention teams can benefit from MobileMap to consult geographical and operational information through GIS services. Moreover, intervention teams can share ground information with decision-makers in command centres who receive this information through the DDSS in the form of photos, audio, texts or maps. Surprisingly, interfaces and functionalities in the proposed systems are not personalised nor flexible or adaptable in case of a change in context. Moreover, the communication of videos is not possible through the system. In addition, the proposed system is oriented for firefighters without taking other involved services into consideration. Eventually, mechanisms related to information confidentiality were not integrated into the proposed system. The third system that we have studied in the literature is MoRep [Ludwig *et al.*, 2013]. MoRep consists of a mobile application oriented for supporting communications in emergency response operations. The focus in MoRep is to ensure a common operational picture and common understanding of situations between off-site units and intervention teams with preventing information overload or lack of information. To this end, the application was proposed on the basis of a semi-structured request-and-report system. Thanks to MoRep, response units can request information, transmit information without requests or transmit information based on previous requests. Moreover, MoRep, allows the response unit to visualise the locations of involved units and information requests. In MoRep, information can be exchanged in several forms such as photos, reports, texts, and videos. The system incorporates users' authentication and access control module which allows the prevention of forbidden access to the system. However, interfaces and functionalities in MoRep are not personalised. Furthermore, aspects related to flexibility and adaptability are not studied in the proposed system.

Other researchers chose to support awareness and communications in rescue and emergency response operations by using ontologies. In this context, several ontology-based systems that aimed at supporting organisational, spatial, and situational information communication were proposed in the literature. For instance, an ontology-based system, called SHARE, was presented and described in [Konstantopoulos *et al.*, 2006, 2008; Velde *et al.*, 2005]. The main objective of SHARE

2.4 Awareness and communication-support systems for rescue and emergency actors

is a common understanding of the situations between different participating actors. It supports multiple functionalities such as Push-to-Share communications, interactive resource management, digital message forms, interactive operation map, and communications indexing and retrieval. Furthermore, SHARE includes automatic speech recognition and text-to-speech module that makes it easy to use by its stakeholders. Thanks to SHARE, final users are allowed to benefit from different functionalities by selecting the appropriate modules based on the user's role and her/his position in the hierarchical level whether it is operational, tactical or strategical. In addition, SHARE is designed in a way that makes it adaptable and flexible through the use of an ontology. Access management mechanisms and other confidentiality mechanisms are also integrated into the system in order to limit the forbidden access to functionalities and information.

A common limitation of these systems is that the communications are limited to organisational, situational, and spatial information while medical and personal information about victims and patients is not considered. Therefore, these systems cannot respond to the diversity of stakeholders' needs.

2.4.3.2 Medical information exchange systems

Mallek *et al.* [2016] proposed an information exchange system to be implemented in French ambulances entitled Communicating ambulance. The objective of this solution was to facilitate exchanges between regulator doctors in hospitals and intervention teams on sites during victims' evacuation and transportation. The proposed system allows the secured exchange of different forms of medical information such as texts, photos, videos, and sensor data. Furthermore, the system was designed in a way that guarantees interoperability between different services and with other systems. In addition, the system is flexible and adaptable for different contexts. For instance, it is possible to adapt the proper channel for communication according to its characteristics such as the form of information to be exchanged and the available bandwidth. Unfortunately, the proposed easy-to-use system does not allow the personalisation and customisation of interfaces and functionalities to different users based on their roles and preferences. Another system was proposed to enhance communication in emergency response and medical evacuation of victims [Nomadec France, 2019]. The aforementioned system consists of medical tablets called Nomadec that bring together communicating medical devices, as well as an innovative application allowing users to efficiently enter and share information related to patients' and victims' management and

2. COMMUNICATION AND SITUATION AWARENESS

evacuation. It also comprises a web application called Nomadeec Telexpert that is oriented for regulator doctors and communicate with Nomadeec. Thanks to Nomadeec and Nomadeec Telexpert, intervention teams can securely exchange different forms of medical information such as texts, photos, videos, and sensor data. This information are then received by regulator doctors in hospitals through Nomadeec Telexpert. The proposed easy-to-use system offers several levels of functionalities that allow each user to find the corresponding items to its competence degree and role. Unfortunately, in our best knowledge, aspects related to adaptability and flexibility are not studied in the design of the system. Another communication system that we will talk about in this context is SINUS that is oriented for large scale emergency response and rescue operations [Séguret, 2013]. This system consists of two main modules. The first one is oriented for intervention teams and allow the fulfilment and classification of victims' general information. Whereas, the second module, called ArcSINUS, enables the reception and integration of information. The advantage of SINUS is that it allows the automatic and secured processing of medical and personal information. Unfortunately, the system requires the use of barcode wristbands. Moreover, SINUS does not allow the personalisation and customisation of interfaces and functionalities. Eventually, SINUS can not be adaptable and flexible to different contexts or any modification in case of need.

A common limitation of these systems is that they focus on medical information without taking into account other important information to be exchanged in rescue operations. Hence these systems do not take into account the diversity of stakeholders' needs. Moreover, these systems are oriented for medical services without taking other involved services such as firefighters into consideration. Hence, they cannot fulfil the criterion that is related to ensuring common operational between different services and actors.

2.4.3.3 Medical, organisational, spatial, and situational information exchange systems

TplSystemes France [2019] proposed a system to support communications in French rescue operations. The system called Pilot Mobile was designed to allow rescuers to visualise and exchange information with decision-makers and doctors that are geographically dispersed. Thanks to Pilot Mobile, rescuers at the intervention sites can benefit from several functionalities such as consulting cartography information, persons' status management, exchanging messages, and

2.4 Awareness and communication-support systems for rescue and emergency actors

transmitting medical records of victims. Different types of information are considered in the system whether it is situational, organisational, spatial or medical. The system is secured through different mechanisms in order to guarantee the confidentiality of information. However, the system is oriented for firefighters without taking medical services into consideration. Furthermore, requirements for information or semantics interoperability are not integrated into the system. Therefore, the proposed system can not fulfil the criterion that consists in ensuring a common understanding and representation of situations between different stakeholders. Furthermore, the proposed system does not allow the personalisation of interfaces and functionalities. Eventually, aspects related to flexibility and adaptability were not studied in the design of the system. In the same context, Elmhadhbi [2020] proposed POLARISC oriented for large scale disasters response in France. The aim of POLARISC is offering to all emergency responders a real-time operational picture among stakeholders by promoting data and semantic interoperability. This ontology-based system consists of an ontology-based messaging service, called PROMES, that performs the semantic translation of the exchanged information. Thanks to PROMES, each stakeholder is able to access information in a specific vocabulary depending on his affiliation. POLARISC also includes a multi-criteria decision support service called PROOVES. Thanks to PROOVES, stakeholders are able to select the most appropriate hospital to the victims' needs during the victims' evacuation process. Except the confidentiality of information, different criteria that a communication and information exchange system oriented for rescue and emergency response are fulfilled by POLARISC. Confidentiality and privacy of personal information are not considered in the system in its current version. Another communication and information exchange system is proposed in France in the context of the NexSIS 18-112 project [Lambert *et al.*, 2019]. The solution consists of cloud-based digital platform to be used by the civilians and the emergency services. It aims at making possible immediate reporting of crisis management at higher levels such as the region or even the nation. NexSIS 18-112 project will be capable of offering video, voice, instant messaging, and real-time text services to emergency stakeholders. In addition, the platform includes the ability to receive information flows produced by social networks and integrate them into the platform. The solution helps to ensure a common operational picture between stakeholders with taking into account the diversity of their needs. It allows the exchange of different forms and types of information. Moreover, aspects related to confidentiality are considered in the solution. However, it is not clear how criteria related to personalisation

2. COMMUNICATION AND SITUATION AWARENESS

of functionalities as well as flexibility and adaptability are fulfilled by the system. This project is still in the development phase and no final results have been published.

2.4.3.4 Discussion and research gaps

Multiple communication and awareness-support systems were developed and oriented for rescue and emergency response operations. These systems were studied and analysed according to the stakeholders' needs and the four identified criteria that a communication system has to fulfil in order to be usable and acceptable by different stakeholders. Unfortunately, in our best knowledge, none of the studied systems respond to all of the needs and criteria and the same time. Table 2.3 shows the classification of the studied systems according to the different stakeholders' needs. As we can see in Table 2.3, only two out of ten systems responds to the diversity of stakeholders' needs. Those systems are POLARISC and NexSIS, which is still a work in progress. Table 2.4 shows the classification of the studied systems according to the different identified criteria. Related to the first criterion that consists in taking into account the diversity of stakeholders' needs, we can see in Table 2.4 that this criterion is barely respected in the proposed systems. Moreover, regarding the personalisation and adaptability to users' contexts, a maximum of five of the studied systems fulfils this criterion. Furthermore, five or six out of ten studied systems do not meet the criterion that consists of flexibility. Eventually, only seven out of ten systems meet the fourth criterion that consists in guaranteeing the confidentiality of information in rescue operations.

2.5 Conclusions

In this chapter, we presented the principal areas and concepts addressed in this research that are awareness and communication. Hence, we started with definitions related to awareness and its different types. A specific type was then presented in detail, which is situation awareness. Models related to this type as well as mechanisms required to improve awareness were described. After that, we examined situation awareness in the domain of rescue operations. Afterwards, we focused on communication and information exchange as a primary key toward reaching awareness. Therefore, we presented an overview of the theory of information communication. We also described problems related to communication and information exchange between different stakeholders in rescue operations. We

then presented some existing studies related to supporting awareness and communications in emergency response and rescue domains. Hence, we showed several existing models that represent and formalise communications and interactions in those operations. Eventually, we presented some systems that aimed at supporting awareness amongst rescue and emergency response actors and evaluated those systems based on stakeholders' needs and four identified criteria. These criteria include: taking into consideration the diversity of stakeholders' needs, personalisation and ease of use even in stressful situations, flexibility and adaptability, and eventually, guaranteeing confidential access to information. The main research gaps drawn from this state of the art were also underlined.

As it has been shown in this chapter, several communication systems already exist and are used by emergency actors inside and outside France. Unfortunately,

Table 2.3: Awareness and communication-support systems and their classification according to stakeholder' needs.

System	1	2	3	4	5	6	7	8	9	10
Exchange of actionable information based on context	X			X		X	X		X	X
Common terminology			X	X	X	X	X		X	X
Interoperable communications between all the services	X		X	X	X	X	X		X	X
Exchange of different required types and forms of information	X	X							X	X
Resources allocation	X	X		X				X	X	X

1:MIKoBOS [Meissner *et al.*, 2006]

2:MobileMap + DDSS [Monares *et al.*, 2011a,b]

3:MoRep [Ludwig *et al.*, 2013]

4:SHARE [Konstantopoulos *et al.*, 2006, 2008; Velde *et al.*, 2005]

5:Communicating Ambulance [Mallek *et al.*, 2016]

6:Nomadeec + Nomadeec Telexpert [Nomadeec France, 2019]

7:SINUS + ArcSINUS [Séguret, 2013]

8:Pilot Mobile [TplSystemes France, 2019]

9:POLARISC [Elmhadhbi, 2020]

10:NexSIS [Lambert *et al.*, 2019]

2. COMMUNICATION AND SITUATION AWARENESS

Table 2.4: Awareness and communication-support systems and their classification according to identified systems criteria.

Criterion	System									
	1	2	3	4	5	6	7	8	9	10
Taking into account the diversity of stakeholders' needs									X	X
Personalisation and adaptation to users' contexts	X			X		X	X		X	X
Flexibility	X			X	X				X	?
Confidentiality			X	X	X	X	X	X		X

1:MIKoBOS [Meissner *et al.*, 2006]

2:MobileMap + DDSS [Monares *et al.*, 2011a,b]

3:MoRep [Ludwig *et al.*, 2013]

4:SHARE [Konstantopoulos *et al.*, 2006, 2008; Veldel *et al.*, 2005]

5:Communicating Ambulance [Mallek *et al.*, 2016]

6:Nomadeec + Nomadeec Telexpert [Nomadeec France, 2019]

7:SINUS + ArcSINUS [Séguret, 2013]

8:Pilot Mobile [TplSystemes France, 2019]

9:POLARISC [Elmhadhbi, 2020]

10:NexSIS [Lambert *et al.*, 2019]

none of those systems has succeeded in responding to all the required criteria for a usable and efficient awareness and communication-support system oriented for rescue actors. For instance, some of them focus on medical information while others give high priority to organisational, situational, and spatial information. In addition, most of the existing systems are oriented for specific emergency services without considering other involved services. For example, some systems are oriented for firefighters while others are oriented for medical services. Moreover, almost all of the existing systems are commercial systems owned by different companies. A direct result of this situation is that the information is heterogeneous; they are stored in distinct data sources with distinct forms and semantics. This heterogeneity results in a deficiency of interoperability between the existing systems. Therefore, it is almost impossible to combine the existing systems into one interoperable system that responds to all of the identified criteria. Similarly, several studies attempted to model practices, interactions, and information flow

in emergency response and rescue operations. Unfortunately, several aspects required in modelling these interactions were not considered in those models. Based on the aforementioned reasons, a real need for implementing a new system that fulfils all the criteria was identified. Therefore, we propose in this thesis an approach for designing Rescue MODES, a system we aim to implement in order to support communications and situational awareness. As mentioned previously in this chapter, semantic representation techniques and ontologies are helpful to respond to the majority of the identified criteria. Furthermore, these techniques are relevant to capture, formalise, and represent the knowledge related to the domain of study. Therefore, we present in the next chapter a detailed description of these techniques as well as existing ontologies related to our research context.

2. COMMUNICATION AND SITUATION AWARENESS

Chapter 3

Knowledge Representation and Ontologies

Contents

3.1	Introduction	54
3.1.1	Historical Background and Definition of Knowledge	55
3.1.2	Knowledge Representation	57
3.2	Ontology	60
3.2.1	Definitions	60
3.2.2	Ontology categories and constituents	64
3.2.3	Ontology languages	67
3.2.4	Ontology development methodologies	68
3.3	Existing Ontologies	70
3.3.1	Ontologies for rescue and emergency response	70
3.3.2	Ontology-based approaches for designing systems and interfaces	76
3.3.3	Ontology-based approaches for access control and rights management	80
3.4	Conclusions	85

3.1 Introduction

In Chapter 2, we identified several criteria that an effective and usable awareness and communication-support system has to meet. These criteria include: Taking into consideration the diversity of stakeholders' needs, personalisation and ease of use even in stressful situations, flexibility and adaptability, and eventually, guaranteeing confidential access to information. Hence, Rescue MODES should be designed in a way that makes it usable by meeting all the identified criteria. Before designing any communication system oriented for a certain domain, it is necessary to capture the knowledge related to the domain and to represent this knowledge through relevant techniques. This will ensure to develop a system that will be accepted by its final users and that it will be appropriate to their practices. To this end, we choose the use of ontologies as an adequate technique to represent knowledge and design the system. The proposed solution is based on three distinct fields of studies. The first field is representing knowledge related to communications in rescue operations. The second one consists of representing the knowledge required for designing the system and its interfaces. Whereas, the third field lies within the representation of knowledge needed for guaranteeing access control and rights management. This chapter of the manuscript aims at setting the context of knowledge representation and presenting the existing related work. We start with historical background about knowledge. We then discuss knowledge representation and focus on ontologies as the selected technique for representing knowledge. Afterwards, we present the definitions of ontologies as well as the most well-known methodologies for building ontologies. Then, we examine and discuss some existing ontologies related to rescue and emergency response domains and we analyse them in terms of ensuring effective communications and enhancing situation awareness. We then move to the literature related to the systems' and interfaces' design part. Hence, we present several ontology-based approaches adopted for designing systems and interfaces as well as existing ontologies developed in this context. Eventually, we move to existing works concerning access control. In this context, several ontology-based approaches developed and applied for access control and access rights management are presented with the corresponding ontologies.

3.1.1 Historical Background and Definition of Knowledge

Our social and economic environment is becoming much more knowledge-driven. This has become a truism to claim that we live in an information society. Yet we've only started to investigate and appreciate the very concrete and daily consequences. The rising value of knowledge is one of these consequences. A brief analysis of the latest research on the Knowledge Society highlights this argument with great intensity. Nowadays, one talks about smart systems, expert systems and networks, and knowledge-based systems. All these terms are generally accompanied by the term Knowledge engineering: The dream to simulate reasoning of human being. Knowledge engineering aims at building knowledge-based systems and expert systems. It consists in modelling the knowledge of a domain in order to operationalise it in a system intended to assist a task or intellectual work in this domain such as problem solving or decision-making [Bachimont, 2004]. The main benefit of this knowledge engineering is that it helps to build systems with the aim of realising problem-solving capabilities comparable to a domain expert [Studer *et al.*, 1998]. Furthermore, it plays the function of a midwife in bringing knowledge forth and rendering it in an explicit way [Sowa, 1999]. Knowledge-based systems constitute one of the most significant technological and commercial descendants of the field recognised as "Artificial Intelligence (AI)" [Schreiber *et al.*, 2000]. Furthermore, their use has various important benefits for businesses and industries. For instance, they help their users to make decisions in a simple and fast way. Moreover, the use of knowledge-based systems helps to increase productivity. Besides, those systems help to enhance the quality of decision making. Therefore, knowledge-based systems tend to increase operational performance in collaborative environments.

The term *knowledge* has caused intellectual debates for over two and a half millennia. Since ancient Greek times, the main interest in philosophy has been to find out what knowledge is. Socrates stirred up some of the greatest conflicts, pretending to learn a least if anything [Sowa, 1999]. Through his constant probing, he undermined the self-confidence of people who appeared to have knowledge and understanding of universal subjects such as justice, beauty, reality, and virtue. Based on the dialectical method of inquiry of Socrates, Plato developed the field of epistemology: A division of philosophy that investigates and studies the origin and nature of knowledge as well as its justification [Stenmark, 2001].

A frequent question that is asked by people in the field of knowledge engineering

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

and representation is: What is knowledge? Knowledge, information, and data are three commonly encountered terms that are closely related, tend to have somewhat different definitions, yet are sometimes used as synonyms for interchangeability, and thus contribute to continuous confusion [Zins, 2007]. Therefore, it is of great importance to make the difference between data, information, and knowledge. The knowledge engineering literature is abundant in various attempts to define data, information, and knowledge and their inter-relationships. A clear distinction between those three terms can be as follows:

- **Data:** Consists of non-interpreted signals that reach our senses [Schreiber *et al.*, 2000]. It is a set of objective and discrete facts about events [Davenport & Prusak, 1998]. A great example of data is the yellow, red, and green light at an intersection. Another example of data is the set of structured records of transactions in an organisational context. Computing devices are full of data such as signals consisting of characters and numbers.
- **Information:** Consists of data with relevance purpose [Davenport & Prusak, 1997]. Schreiber *et al.* [2000] defined information as data equipped with meaning aiming at describing a condition or a situation. An example of information can be the emergency alert. For a firefighter operator, the sound of an alarm is not just an audio signal, rather, it is interpreted as an indication to react.
- **Knowledge:** Consists of the entire body of information and data that individuals put to bear for actual use in their practices in a way to carry out projects and to generate new information [Schreiber *et al.*, 2000]. Wiig [1994] defined knowledge as a set of beliefs, judgments, truths, perspectives, and methodologies. Hence, knowledge contributes to different aspects: first a generative capability, since knowledge is capable of producing new information; second a sense of purpose, because knowledge is intellectual machinery used to reach an objective. Therefore, it is inevitable that knowledge is declared to be the factor of production and growth.

The relationships between the three terms are described as a hierarchy starting with data, followed by information, and with knowledge on top [Ackoff, 1997; Choo *et al.*, 2013; Stenmark, 2001]. Figure 3.1 represents the data, information, and knowledge model. As we can see in Figure 3.1, the relationship between the three terms is asymmetrical implying that the data can be converted into information that can be converted into knowledge. Furthermore, it can be asserted

that knowledge is more valuable than information that is superior to data. In addition, knowledge depends on the context. For instance, one person's data can be considered as knowledge for another person. Hence, the borderlines between knowledge, information, and data are not clear since they are relative to the context of use. The observation of the knowledge dependency on context can be contained in different terminology across the different use of knowledge. In knowledge engineering, it has been common to find that knowledge is an essential task and domain-specific [Schreiber *et al.*, 2000].

3.1.2 Knowledge Representation

The term *representation* is philosophically vexing as that the term *knowledge*. Generally speaking, representation is a relation between two domains where the first is supposed to back up or take place of the second. Typically, the first one, the representative, is in any manner more specific, real or available than the second [Brachman & Levesque, 1986]. For instance, printing a hamburger and a soda bottle on board could point out a less visible fast food restaurant. Plato's student, Aristotle, moved the priority of philosophy for the origin of knowledge to the minor conversational, yet a more realistic problem of representing

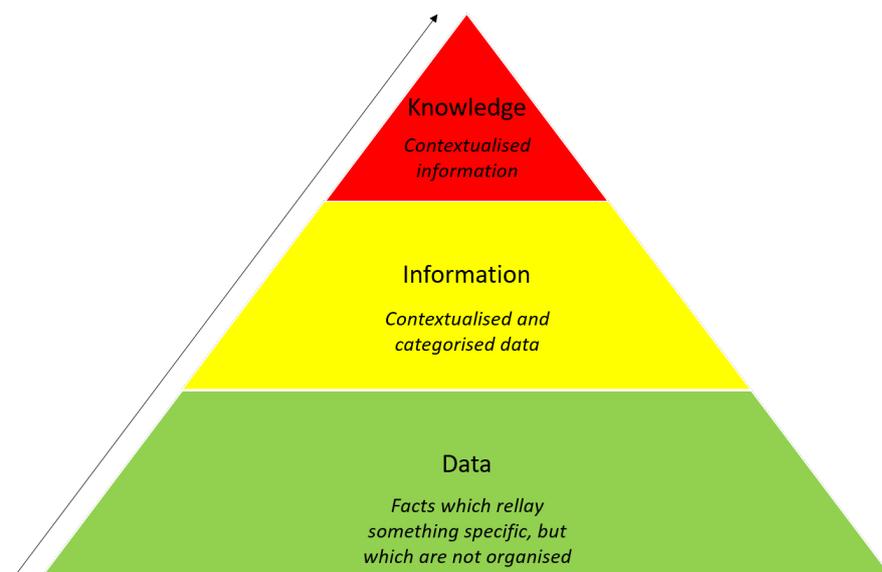


Figure 3.1: Hierarchy of data, information, and knowledge.

*Figure adapted from [Mutongi, 2016].

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

knowledge. In this context, he defined the scopes and provided the initial terminologies of ethics, linguistics, physics, biology, metaphysics, logic, psychology, politics, and economics. For all of those areas, the words he has either adapted or created have become the centre of today's international technological vocabulary. Developed as a branch of artificial intelligence, knowledge representation helps to develop computer programs that are the basis for a machine-readable depiction of the world [Grimm, 2009]. Sowa defined knowledge representation as the use of ontologies and logic to build computable models in a domain [Sowa, 1999]. Without logic, the representation of knowledge is ambiguous since the criteria for determining whether arguments are inconsistent or conflicting will no longer exist. In logic, the existential quantifier is a notation of the existence of something. Yet reasoning itself does not provide a language to describe the things that exist. This gap is filled by ontologies that make it possible to study and represent the existence of all kinds of entities that compose the world whether they are of abstract or concrete nature [Sowa, 1999]. Therefore, knowledge representation is a multidisciplinary topic that applies hypotheses and strategies for three other fields [Sowa, 1999]:

- **Logic:** Defines the conceptual framework and rules of reasoning
- **Ontology:** Defines the kind of nature and origin that exist a certain domain
- **Computation:** Supports the technologies that differentiate knowledge representation from pure philosophy

There are various methods to analyse and study the field of knowledge representation. We may think of it from a representational language point of view like that of symbolic logic, and focus on how logic can be extended to problems in artificial intelligence. This has led research and studies in what is referred to as "logic-based Artificial Intelligence". Artificial intelligence consists of the analysis of cognitive actions and human behaviour accomplished by computational methods. Therefore, knowledge is relevant for AI systems due to many reasons since it is always necessary to describe the behaviour and actions of complex systems whether they are human or not using terminology that contains terms such as "objectives", "intentions", "thoughts", and "hopes" [Brachman & Levesque, 1986; Rastier, 1995]. Identifying such a terminology necessitates the careful analysis of the nature of objects and entities as well as the relations that can exist in a domain. Moreover, the representation terminology includes a set of concepts that describe the facts of a certain domain, whereas the body

of knowledge which uses that terminology is a compilation of facts about the domain [Chandrasekaran *et al.*, 1999]. To enhance the exchange and reuse of formally expressed knowledge across AI systems, it is useful to identify a common terminology through which exchanged knowledge is represented. The development of a representational terminology for a certain domain including concepts, functions, and relations is called an ontology [Gruber *et al.*, 1993]. Another technique for representing knowledge and defining domain terminology is the use of conceptual graphs that allow a visual definition of concepts and relations [Sowa, 2008]. Conceptual graphs are graphical representations for reasoning based on the existential graphs of Charles Sanders Peirc [Roberts, 1992] and the semantic networks of artificial intelligence [Sowa, 1987]. In addition to the four previous techniques, knowledge can be represented through rules that reflect the notion of consequence. Rules come in the form of if-then constructs that allow complex derivation statements to be articulated [Grimm, 2009].

On the other hand, it is possible to study the technique of knowledge representation in terms of the design and development of knowledge-based systems [Brachman *et al.*, 1991]. Several researchers state that the use of knowledge representation techniques such as ontologies would facilitate the knowledge engineering process [Van Heijst *et al.*, 1997]. In Artificial Intelligence, ontologies have been established to enable the exchange and re-use of knowledge. The explanation of why ontologies are becoming so prominent is primarily due to what they promise: a mutual and shared comprehension of a domain that can be conveyed between people and application systems [Fensel, 2001]. Another important role of ontologies is facilitating the construction and formalisation of a domain model by providing the required terminology of terms and relations. This will allow the description and representation of the static domain knowledge of a knowledge-based system [Fensel, 2001]. In a knowledge base, ontologies describe the nature and categories of entities that exist or may occur in the domain of application [Sowa, 1999]. Furthermore, the use of ontologies is beneficial since they provide a machine-processable semantics of information sources that can be communicated between humans and software [Fensel, 2001]. Therefore, ontologies incorporate two main aspects that help to push a knowledge-based system to its maximum potential [Fensel, 2001]:

- Describing structured knowledge semantics that enable the processing of information by a machine

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

- Describing semantics that connect human interpretation of knowledge with machine-processable information based on agreed terminology

However, the nature of an ontology forbids it from being directly applicable to specific contexts and domains [Studer *et al.*, 1998]. Ontologies need to interweave the machine interpretability of symbols with their human interpretation. Hence, it is important to investigate the nature of ontologies and the ways they can provide the appropriate functionalities and services.

3.2 Ontology

The growing need for machine and human agents to obtain and share knowledge in a precise and effective manner has contributed to more and more use of ontologies, web services, and the fusion of both, i.e. semantic web services [Berners-Lee *et al.*, 2001], for the sharing of knowledge. During the last decade, ontologies have become common research subject to many artificial intelligence researchers including natural language processing, knowledge representation, and knowledge engineering. More recently, the notion of ontology has evolved to other fields such as knowledge management, information retrieval, and intelligent information integration. In this section, we investigate the definitions of ontologies from a philosophical and artificial intelligence point of view. We then discuss the importance of using ontologies as a relevant technique for representing knowledge and designing knowledge-based systems.

3.2.1 Definitions

The term “ontology” derives from Greek, with “logos” meaning “science” and “onto” usually interpreted as “being” so that ontology is traditionally understood as the science or study of being [Lawson, 2004]. This definition stretches as far back as Aristotle’s effort to explain and describe the existence of entities throughout the universe [Studer *et al.*, 1998]. There have been several interpretations of ontologies over the last decade. From a philosophical point of view, it is always said that ontologies “*carve the world and its joints*” [Chandrasekaran *et al.*, 1999]. This means that an ontology consists in studying the nature and origin of things that make up the universe including objects, relations, processes, and events [Sowa, 1999]. Philosophers always use the term “ontology” as a synonym of “metaphysics”, a word used by some of Aristotle students to refer to

what is called “first philosophy”. In some cases, the word “ontology” is used in a wider context to refer to the analysis of what *might* exist and can be expressed in one question: What is there? The answer is everything [Smith, 2003].

Ontologies aim at classifying the entities in all spheres of being in an exhaustive and definitive way [Smith, 2003]. By exhaustive it is meant that the classification includes all the categories and types of entities as well as the relations by which those entities are linked together to form larger wholes. Whereas, descriptive means that the classification should be accomplished in a way that makes it able to answer multiple questions such as: What classes of entities are needed for a full explanation and description of all the events in the world? Or: What are the required classes to provide an account of what makes true all truths?

Unlike the experimental sciences, which seek to explore and model life under a certain viewpoint, ontology focuses on the essence and function of objects independently of all other factors, and regardless of their actual existence [Guarino *et al.*, 2009]. For instance, it could happen to study the ontologies of imaginary entities such as unicorns. This means that their nature and structure can be expressed in terms of general terms even though they do not exist in reality.

On the other hand, ontologies were studied and used in the fields of computer sciences especially in artificial intelligence. In this case, ontology is referred to as a specific type of computational artefact or information object. Artificial intelligence researchers used the term ontology to define and describe what could be represented of the universe in a computational program [Studer *et al.*, 1998]. Several definitions of ontologies were provided in the last decade in the field of artificial intelligence. In this context, a first definition was provided in 1993 by Gruber who defined ontology as “*an explicit specification of conceptualisation*” [Gruber *et al.*, 1993]. A more recent definition was given by Borst in 1997 where ontology was defined as “*a formal specification of a shared conceptualisation*” [Borst *et al.*, 1997]. Based on this definition, it is required that the conceptualisation reflects a common understanding and view between several parties rather than a singular view. This conceptualisation may also be represented in a machine-readable format [Guarino *et al.*, 2009]. In 1998, Studer *et al.* [1998] defined the term ontology by merging the two previous definitions. Hence, they stated that an ontology is “*a formal, explicit specification of a shared conceptualisation*”. In the latter definition, one has to focus on three major aspects:

- The meaning of conceptualisation: Conceptualisation is referred to as an abstract, simplified model of some phenomenon in the world that is repre-

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

sented for some purpose by having identified its pertinent concepts [Studer *et al.*, 1998]. This model constitutes the backbone of any formal representation of knowledge. Furthermore, every knowledge-based system is based on some conceptualisation either directly or indirectly [Gruber, 1995].

- The meaning of proper formal, explicit specification: Explicit means that the type of the identified concepts should be explicitly defined together with the restrictions of their use. For instance, in medical fields, the most used concepts are symptoms and diseases, the relationship between them is causal, and the restriction is that the disease can not cause itself [Studer *et al.*, 1998]. Whereas formal means that the ontology must be machine-processed and readable [Guarino *et al.*, 2009].
- The importance of “shared”: The aspect of sharing was introduced to the definition of ontologies by Borst in 1997 [Borst *et al.*, 1997]. Sharing requires that the ontology captures collective knowledge, that is not a specific individual perception of the target phenomenon, but one embraced by a community [Studer *et al.*, 1998].

Based on the given definitions, ontologies have great importance as a technique for formalising and representing knowledge in a certain domain. Moreover, they serve as a basis for constructing systems that are based on this knowledge. Ontologies analysis plays a vital role in defining the structure of knowledge and formalising it. For instance, given a certain domain, its ontology constitutes the central basis of every system of knowledge representation related to that domain. As mentioned in the previous section, the absence of ontologies or conceptualisations that express knowledge may result in the absence of vocabulary for representing knowledge. Moreover, a weak ontological analysis leads to inconsistent knowledge bases. Therefore, a key first step toward the development and creation of efficient vocabularies and knowledge representation systems consists in performing an efficient ontological study of the target domain. Another important reason that makes the use of ontologies beneficial lies within the fact of allowing knowledge sharing [Chandrasekaran *et al.*, 1999]. Suppose that we make the ontological analysis for the domain of rescue and construct a related ontology. The resulting ontology will surely include general concepts such as persons, vehicles, and material; domain-specific concepts such as rescuers, victims, and incidents; and terms that describe a situation such as a medical situation. Those terms should be associated with the relations and concepts in the ontology to

build a knowledge representation language of the domain. Besides, a syntax for encoding knowledge in terms of those concepts and relations should be devised. Once done, this knowledge representation language can be shared with other individuals who share similar desires without the need for repeating the knowledge analysis process. Hence, shared ontologies constitute the basis for domain specific knowledge representation languages and interoperability between different systems [Chandrasekaran *et al.*, 1999]. Moreover, ontologies are designed to be used in systems that need to interpret the content of information and to reason about it rather than merely presenting information to users. In this context, they allow better interpretability of content than that provided by other techniques and languages such as XML and RDF Schema by supplying formal semantics along with additional vocabulary [Valls *et al.*, 2010]. According to [Studer *et al.*, 1998], ontologies have a similar function to that of a database schema with the following differences:

- The information presented by an ontology consists of semi-structured language that is interpretable by humans and machines.
- Ontologies are constructed using language that is richer in semantics and syntax than the common approaches for databases.
- Ontologies provide a domain theory instead of providing the structure of a data container.

To summarise, the reasons that justifies the use of the ontological approach are provided as follows:

- Ontologies allow the specification of semantic relations between various concepts.
- Ontologies enable a common understanding of knowledge among different entities whether they are humans or software agents, which enables the information to be reasoned and processed automatically.
- Ontologies are flexible and able to be reused over time.
- Ontologies are exchanged between various actors, which helps to address interoperability issues.

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

3.2.2 Ontology categories and constituents

Several classifications of ontologies were presented in the literature to differentiate their different categories [Asunção *et al.*, 2004; Falquet *et al.*, 2011; Guarino, 1998; Lassila & McGuinness, 2001; Van Heijst *et al.*, 1997]. One of the most used classification methodologies are those that are based on domain scope as it has been done in [Falquet *et al.*, 2011; Guarino, 1998; Van Heijst *et al.*, 1997]. Falquet *et al.* [2011] classified ontologies based on domain scope into five categories, each having its specifications and use cases. These categories depend on the level of generality of the ontology. Figure 3.2 represents the classification of ontologies as given in [Falquet *et al.*, 2011]. As we can see in Figure 3.2, ontologies are separated into top-level ontologies, also called foundational ontologies, core reference ontologies, domain ontologies, task ontologies, and application ontologies.

- **Top-level or foundational ontologies:** They can be viewed as generic or meta-level ontologies that can be applied to different domains independently of a specific domain or problem. They define general concepts used to construct other ontologies such as processes, events, objects, relations, and many other high-level concepts. The main advantage of using foundational ontologies is to guarantee the interoperability between different domain ontologies and to facilitate the reuse and integration of knowledge [Masmoudi *et al.*, 2020]. The most well-known top-level ontologies are the Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE) [Gangemi *et al.*, 2002], the Suggested Upper Merged Ontology (SUMO) considered as the largest accessible ontology [Pease *et al.*, 2002], and the Basic Formal Ontology (BFO) [Arp *et al.*, 2015].
- **Core reference ontologies:** Also called mid-level ontologies, they are a

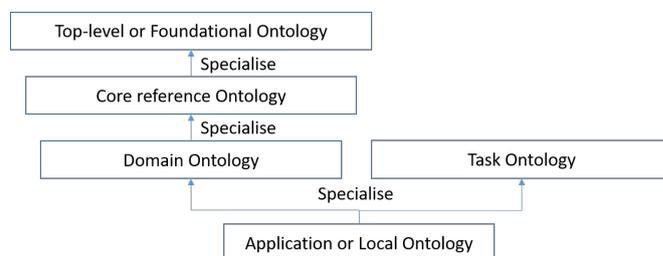


Figure 3.2: Ontologies classification based on domain scope.

*Adapted from [Falquet *et al.*, 2011].

specification of top-level ontologies that capture the central concepts and relations of a domain and constitute a standard used by different group of users [Masmoudi *et al.*, 2020]. Although mid-level ontologies are linked to a domain, they integrate various viewpoints related to a specific group of users. A well-known example of mid-level ontologies is the collection called Common-Core ontologies [Schoening *et al.*, 2015]. Other examples of core reference ontologies are the Hydontology ontology created to describe the hydrographic features [Blázquez *et al.*, 2007] and the Customer relationship domain ontology [Magro & Goy, 2012].

- **Domain ontologies:** They are specification of top and mid-level ontologies and describe the vocabulary related to a specific area of knowledge. In contrast to mid-level ontologies, domain ontologies apply to a generic domain such as crisis management or rescue operations with a particular point of view [Masmoudi *et al.*, 2020]. Domain ontologies can also be specialised in order to build application ontologies that describe specific concepts in a particular domain and particular associated tasks. Good examples of domain ontologies are those related to crisis management and emergency response domain [Yu *et al.*, 2008] or ontologies for medicine and biomedical domains such as the Biodynamic Ontology, which is a domain ontology based on the BFO foundational ontology [Grenon *et al.*, 2004].
- **Task ontologies:** They provide specific concepts for particular tasks in a given domain. For instance, the concept “protection” belongs to the rescue task ontology. Task ontologies help to solve interaction problems by providing a reasoning point of view on domain knowledge [Studer *et al.*, 1998]. Furthermore, they allow making explicit interaction between domain knowledge and problem-solving through assumptions [Benjamins *et al.*, 1996]. Examples of task ontologies are the Task Ontologies for GeoVisualisation [Fabrikant, 2001] and the ontologies of tasks for emergency response operations [Li *et al.*, 2008; Wiegand & García, 2007].
- **Application or local ontologies:** They are a specialisation of the domain and task ontologies and occupy the lowest level in ontology categories. Application ontologies are used in order to fulfil the specific purpose of an application in a given domain [Fonseca *et al.*, 2000]. It is therefore a question here of relating the concepts linked to a particular task in order to describe its execution. Many application ontologies have been built in the

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

context of systems oriented for crisis management and emergency response. Well-known application ontologies in this context are the EMERGEL ontology [Casado *et al.*, 2015], EDXL-RESCUER [Barros *et al.*, 2015] and SHARE-ODS [Konstantopoulos *et al.*, 2006] developed to support DISASTER [Schütte *et al.*, 2013], RESCUER [Villela *et al.*, 2014] and SHARE projects respectively [Konstantopoulos *et al.*, 2006].

Whatever the category of the ontology is, each ontology has a set of constituents in a way that makes it usable and interpretable. According to [Lord, 2011], a computational ontology consists of a disjoint set of core components that are concepts, individuals, relations. Also so-called universals, concepts are a core component of most ontologies. They represent a set of different real-world entities that share common characteristics and features. For example, mammals share certain common characteristics such as a set of specific body parts and related DNA. In an ontology, concepts are classes organised in one or multiple taxonomies, linked through transitive is-a relationships. In addition, multiple inheritances are supported in most ontology languages. This means that each concept can have several hierarchical subsumers or ancestors [Valls *et al.*, 2010]. Moreover, some languages allow the classification of concepts extensionally by their membership. For instance, the concept “Members of intervention team” can be defined as the set of “George, Emmanuel and Michael”. As being said, each concept is a group of different real-world entities called individuals. Individuals, also known as particulars or instances, form the central unit of an ontology [Lord, 2011]. They constitute the way of describing the entities of interest. Individuals can represent abstract objects like information and situation, or concrete objects like vehicles, persons, and instruments. In general, an individual can be an instance of multiple concepts at the same time. However, it is possible to specify that two or more concepts are disjoint, which means that the instances of one concept cannot be instances of the others [Valls *et al.*, 2010]. The third core component of an ontology consists of relations. Relations are binary associations between concepts. In this case, the concept in the origin of the relation is called the domain whereas the concept in the destination represents the range [Valls *et al.*, 2010]. Relations can also be expressed directly between individuals to link them with each other [Lord, 2011]. There exist two types of relations: domain-dependent relations; and relations that are common to any domain. In addition to the three core components, some ontologies incorporate two more constituents that are attributes and data types. Attributes reflect the qualitative

and quantitative characteristics of some specific concepts, which have values in a given context identified by the data type [Valls *et al.*, 2010].

3.2.3 Ontology languages

To make ontologies available to information systems, they have to be constructed and implemented using standardised ontology languages [Grimm, 2009]. Over the last few years, several languages for developing and querying ontologies and knowledge bases have been developed. The majority of these languages is based on the eXtensible Markup Language (XML) [Bray *et al.*, 1997] which allows them to be interpretable and processed in computers and machines [Munir & Anjum, 2018]. Well-known ontology languages are the Resource Description Framework (RDF) and RDF Schema [McBride, 2004], the Ontology Web Language (OWL) [Bechhofer *et al.*, 2004] and OWL-2 [Motik *et al.*, 2009], and the DARPA Agent Markup Language and the Ontology Inference Layer (DAML + OIL) [Gómez-Pérez & Corcho, 2002]. Amongst these languages, the most used are RDF and OWL [Valls *et al.*, 2010]. Both RDF and OWL have several similar characteristics. However, OWL is a stronger language with more computer interpretability Munir & Anjum [2018]. Besides, OWL comes with greater vocabulary and simpler syntax than RDF, which is beneficial to define complex ontology inferences and restrictions [Munir & Anjum, 2018]. OWL is composed of three sublanguages: OWL-Lite, OWL-DL, and OWL-Full. It has been built on top of RDF and DAML + OIL, which has steadily increased its expressiveness [Munir & Anjum, 2018]. To improve the expressiveness of OWL, other languages can be integrated with OWL such as the Semantic Web Rule Language (SWRL) [Horrocks *et al.*, 2004]. SWRL applies rules to OWL-DL and OWL-Lite and is a mixture of the OWL sublanguages and the Rule Markup Code sublanguages. OWL-2 is an updated version of OWL-1 and has been developed based on the existing structure of this latter [Motik *et al.*, 2009]. Moreover, all the building blocks of OWL-1 are present in OWL-2. Hence, every OWL-1 ontology is a valid OWL-2 ontology [Munir & Anjum, 2018]. OWL-2 differs from OWL-1 by adding three new profiles: OWL-2-EL, OWL-2-QL, and OWL-3-RL. Each OWL-2 profile can be selected based on the ontology structure and the reasoning tasks.

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

3.2.4 Ontology development methodologies

To develop an ontology, it is of great importance to adopt a methodology that manages and guides the development process. Indeed, the selected development methodology may extremely affect the efficiency of an ontology. Several methodologies for the design and development of ontologies have been proposed in the literature. Several studies were conducted to analyse the different methodologies [Corcho *et al.*, 2006; Jones *et al.*, 1998; Karray *et al.*, 2012; Mizoguchi, 2004]. From those methodologies, one can cite METHONTOLOGY, On-to-Knowledge, Toronto Virtual Enterprise (TOVE), the Activity First Methodology (AFM), and the Unified Process for Ontology Building (UPON) Methodology.

- **METHONTOLOGY:** It was proposed by at Polytechnic University of Madrid [Mizoguchi, 2004] and is considered as one of the commonly used methodologies for ontology development [Falquet *et al.*, 2011]. METHONTOLOGY consists of multiple activities that are classified into management activities, development activities, and support activities. Regarding the development activities that constitute the core of the methodology, they consist of five steps that are respectively: (1) Specification; (2) Conceptualisation; (3) Formalisation; (4) Implementation; and (5) Maintenance [Fernández-López *et al.*, 1997]. This approach stresses the re-use of current domains and upper-level ontologies to facilitate the development phase and to enhance the interoperability between ontologies [Falquet *et al.*, 2011].
- **On-to-Knowledge:** It is oriented specifically for knowledge management applications [Karray *et al.*, 2012]. This methodology was provided by several researchers at Karlsruhe University to introduce and maintain ontology-based knowledge management. The proposed methodology is based on a two-loop architecture: Knowledge process and knowledge meta-process. Knowledge process means a normal use of knowledge whereas knowledge meta-process is the methodology of ontology development and consists of five main steps: (1) Feasibility study; (2) Kickoff; (3) Refinement; (4) Evaluation; (5) Application [Mizoguchi, 2004]. According to this approach, significant emphasis should be based on the physical presence of the targeted domain experts, brainstorming processes, and specialised technologies to promote ontological development [Cristani & Cuel, 2005].
- **Toronto Virtual Enterprise:** It was created to assist business process modelling at the University of Toronto. This methodology is the most sys-

tematic of the existing ones. A key first step in this methodology consists in listing the questions to be addressed by the corresponding ontology and presenting them in a systematic formal vocabulary to use them for ontology testing [Karray *et al.*, 2012]. Its competency questions approach is well-accepted and adapted in other methodologies such as On-to-knowledge [Mizoguchi, 2004].

- **Activity First Methodology:** It is dedicated to the development of task ontologies. One of the core ideas in this methodology is that task ontology provides users with a collection of roles played in a task context by using domain concepts [Mizoguchi, 2004]. A mandatory first step in this methodology is the selection of the source documents from which the ontology will be extracted [Mizoguchi *et al.*, 1995]. This methodology consists of four other steps as follows: (1) Extraction of task units; (2) Organisation of task-activities; (3) Analysis of task structure; (4) Organisation of domain concepts [Mizoguchi, 2004].
- **Unified Process for Ontology Building Methodology:** It takes advantage of the Unified Process (UP) and the Unified Modelling Language (UML) [De Nicola *et al.*, 2009]. Oriented for the development of large-scale ontologies, UPON is use-case driven since it does not aim at building generic domain ontologies. However, it is specific for ontologies that serve its users in a well-defined application area with accurately defined goals. The proposed methodology is of iterative and incremental nature and consists of four parameters: Cycles, phases, iterations, and workflows. Each cycle includes four phases that are inception, elaboration, construction, and transition. Moreover, each phase is divided into several iterations where five workflows take place: requirements, analysis, design, implementation, and test. We notice that this methodology requires the involvement of domain experts and knowledge engineers in the development phase.

Each one of those methodologies has its requirements and context of use. However, they are generally similar and share resembling procedures and steps. The five widely recognised steps for developing an ontology are Specification, Conceptualisation, Formalisation, Implementation, and Evaluation [Pinto & Martins, 2004].

3.3 Existing Ontologies

As it has been mentioned in Chapter 1, we propose in this thesis an ontology-based approach for designing a communication system oriented for rescue operations. This approach includes the integration of an access control policy to guarantee the confidential access to information in the system to develop. In addition to the communication and interaction aspects, it is essential to address design and access control aspects. In this section, we present existing works related to ontologies for rescue and emergency response as well as ontology-based approaches for designing systems and interfaces and guaranteeing access control.

3.3.1 Ontologies for rescue and emergency response

Related to our purpose, several works have been distinguished in the context of knowledge engineering to build crisis and emergency response systems such as knowledge-based models proposed to support environmental emergency management [Hernandez & Serrano, 2001], or models to solve unconventional emergencies problems by using domain knowledge and ontologies [Feng *et al.*, 2016]. Furthermore, several ontology-based systems were developed to support awareness, information exchange, and communication in rescue and emergency response operations. To this end, multiple domain, task, and application ontologies were proposed in these domains. Moreover, several domain and application ontologies were constructed in the context of crisis management and large-scale disasters response domain to support decision-makers. In this section, we present and analyse several recent ontologies oriented for crisis management, emergency response, and rescue domains. Javed *et al.* [2011] proposed an ontology-based system to support team situation awareness by unifying situation understanding between participants. The proposed system has an inference agent designed to use the profile information of the members of the team, such as roles, assignments, and their specifications and interdependencies, to provide them with the right information at the right time. To this end, an application ontology has been proposed. The constructed ontology is composed of five modules respectively: Spatio-temporal, Task, Personal, Social, and Environmental. However, the obtained ontology does not include concepts related to victims and medical information. Furthermore, the aforementioned ontology is not publicly accessible. A similar system that sought to enhance information sharing and coordination was proposed in the context of the DISASTER project [Schütte *et al.*, 2013]. This project is based

on a modular common ontology called EMERGEL ontology [Casado *et al.*, 2015] constructed for this aim. This application ontology is constructed to temporally describe a crisis by defining different modules divided into transversal modules and vertical modules. To construct this ontology, authors chose to specify some top-level classes defined in the generic ontology DOLCE [Gangemi *et al.*, 2002]. Transversal modules are time and space while vertical modules are objects representing concepts in the real world, constructs representing a set of objects, and activities representing tasks to be achieved by objects and constructs. Each one of these modules is divided into many classes. For example, objects contain Person, Vehicle, Equipment, Infrastructure, and SpatialPoint. However, this ontology lacks some specific aspects related to communication. For instance, specific operational information such as the availability of resources is not considered in the ontology. The proposed ontology can be useful for decision-making purposes at the strategic level of operations rather than the operational levels. Another application ontology called POLARISCO was proposed in the context of the POLARISC system that aims at enhancing semantic interoperability between French emergency response organisations in disaster response Elmhadhbi *et al.* [2019]. To build the proposed ontology, the authors adopted METHONTOLOGY [Fernández-López *et al.*, 1997] and reused BFO [Arp *et al.*, 2015] as a top-level ontology as well as Common Core Ontology as mid-level ontology [Rudnicki, 2017]. The proposed ontology includes a common module, a message module, and five other modules different each oriented for a specific organisation. This ontology has the advantage to cover several important aspects in crisis and disaster response ranging from involved organisations to persons and their roles, passing by means and infrastructure. Unfortunately, in its current version, the proposed ontology does not show how different tasks are related to their requirements in terms of information, which is essential for operational and communication aspects. Another application ontology called EXDL-RESCUER [Barros *et al.*, 2015] was created to support the RESCUER project [Villela *et al.*, 2014], which uses crowd-sourcing information to assist actors in emergencies. This application ontology is based on Emergency Data Exchange Language (EDXL) and aims at constructing a conceptual model that corresponds to information exchange and coordination with other systems. It focuses on the type of exchanged information and it covers a group of message contexts in an emergency. In this ontology, authors defined twelve concepts related to the type of shared messages during an emergency response such as Alert, Info, ResponseType, and MsgType. However, the focus in this ontology is mainly on alerting people. A similar ontology was proposed

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

in [Chan *et al.*, 2017]. Called the Public Safety and Emergency Management (PS/EM) Communication ontology, this ontology was developed by the Institute for Defence Analyses (IDA). To this end, authors based their work on EDXL standards including alerting protocol, resource messaging, hospital availability exchange, and messaging distribution element. The ontology was constructed by specifying the BFO and Common Core Ontologies. However, this ontology does not cover all types of communication between emergency response organisations and actors, it is focused on alert messages. On the other hand, several domain ontologies have been developed in the domain of crisis, rescue, and emergency response. Yu *et al.* [2008] developed a domain ontology that aimed at supporting knowledge reorganisation in decision support systems. The proposed ontology was constructed based on emergency response documentation by adopting the Activity First Methodology [Mizoguchi *et al.*, 1995]. They defined four main classes: EVENT that can be a disaster or disease, RESOURCE made of artificial and in-artificial, SUBJECT divided into personal and actor, and TASKS consisting of “communication”, “evaluation”, “rescue”, “prevention”, and “detection”. Each one of these classes is also divided into different subclasses, each having several instances. In the domain of rescue operations, this ontology can serve by giving the general concepts that are in common with crisis management. This ontology has the advantages to cover different contexts in emergency response. Unfortunately, the development of this ontology was limited to the construction of an is-a taxonomy without defining relations between different concepts. Another domain ontology related to crisis management called IsyCri was proposed in [Bénaben *et al.*, 2008]. The aforementioned ontology was built to support Isycrri, a French project designed to allow the interoperability between different organisations involved in crisis management [Bénaben *et al.*, 2016]. The proposed ontology structures and formalises concepts related to disaster response. Unfortunately, the proposed ontology is not publicly accessible nor downloadable. For a better management of emergencies, authors in [Santos *et al.*, 2019] propose the use of models representing detailed knowledge about the types of adverse events and their consequences. To this end, the basic formal infrastructure incident assessment ontology (BFiaO) was built based on the Coordination of Emergencies and Tracking of Actions and Resources (CESAR) taxonomy. CESAR which provides an exhaustive taxonomy of events, actions, and resources required to achieve operations in emergency field. However, concepts related to victims and medical information are neither considered in BFiaO nor CESAR. Similarly, Nunavath *et al.* [2016] proposed representing knowledge related to fire

emergency response through a domain modelling approach. To this end, a domain ontology called Building Fire Emergency Response (BFER) ontology was proposed. To build BFER, Nunavath *et al.* [2016] adopted the METHONTOLOGY methodology. BFER describes the knowledge that can be used by firefighters inside the building during rescue operations. It consists of four components: an actor components, an event component, an event component, and a building component. Unfortunately, the proposed ontology and the obtained model do not take the operational practices of actors into consideration. In the same context, Bannour *et al.* [2019] propose the Crisis Response Ontology (CROnto) that defines crisis features, effects, and response. CROnto formalises knowledge related to disasters and their damages, resources, and organisations. However, concepts related to victims, personal, and medical information are not considered in this ontology. Moreover, the focus is on contributing to strategic planning more than operational response. Another domain ontology for emergency response and management called the Emergency Response Ontology (EMO) was presented in [Fan & Zlatanova, 2011]. EMO aimed at solving the problems of semantic data heterogeneity in emergency response and their transmission to stakeholders. It is composed of two parts: a static data ontology and a dynamic data ontology. It is also linked to several domain ontologies that define the stakeholders' knowledge. Unfortunately, the ontology is not downloadable. One more proposed ontology in this context is the Management of a Crisis Vocabulary (MOAC). MOAC is a lightweight vocabulary that defines terms for linking crisis information from three different sources: traditional humanitarian agencies, volunteer and technical committees, and disaster affected communities. MOAC defines crisis types, response activities, damages, and victims. However, it does not describe specific resource types. Moreover, concepts related to communication are not defined in this ontology [Limbu *et al.*, 2012]. Similarly, multiple task ontologies have been proposed for the domain of rescue and emergency response. Li *et al.* [2008] proposed a task ontology to support the implementation of the evacuation planning system for emergency cases and to standardise a group of semantic concepts used in different emergency systems. It defines a common vocabulary usable by emergency actors regardless of the emergency nature. To build this ontology, the authors identified four generic concepts that are Response Preparation, Emergency Response, Emergency Rescue, and Aftermath Handling. Each one of these concepts is divided into several sub-concepts, illustrating the main steps and tasks to be taken in case of an emergency. This ontology is restricted to a taxonomy of the main tasks to achieve during an emergency case. Those tasks are not linked to

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

different roles or requirements. In the same context, Wiegand & García [2007] proposed the use of a task ontology to build an ontology-based system capable of retrieving geospatial data automatically in emergency response. The proposed system aimed at providing relevant results to users who search for data when achieving tasks such as planning activities. To this end, the authors created an ontology of tasks as well as ontology of data sources. They also defined the relations between tasks and data sources. Data sources cover different types of organisational, spatial, and situational information. We notice that medical and personal information were not considered in this work.

As it has been presented in this section, multiple domain, task, and application ontologies were proposed in the domains of crisis management, emergency response, and rescue operations. Table 3.1 shows a summary of the analysed ontologies that were developed to formalise knowledge related to those domains.

Table 3.1: Existing ontologies for rescue, emergency response, and crisis management domains.

Ontology	Contribution	Reference
Emergency response application ontology	Representing knowledge and unifying situation understanding in emergencies	[Javed <i>et al.</i> , 2011]
EMERGEL ontology	Defining concepts for temporally describing a crisis situation	[Casado <i>et al.</i> , 2015]
POLARISCO	Enhancing semantic interoperability between French organisations in large-scale emergencies	[Elmhadhbi <i>et al.</i> , 2019]
EXDL-RESCUER Ontology	Constructing a conceptual model of information exchange and coordination with other systems	[Barros <i>et al.</i> , 2015]
PS/EM Communication ontology	Representing information sharing standards between PS and EM entities	[Chan <i>et al.</i> , 2017]
Emergency response domain ontology	Constructing an is-a taxonomy for concepts used in emergency response	[Yu <i>et al.</i> , 2008]

3.3 Existing Ontologies

IsyCri Ontology	Structuring and formalising knowledge and concepts related to disaster response	[Bénaben <i>et al.</i> , 2008]
BFiaO	Providing a model that covers high-level aspects in handling infrastructure-related situations	[Santos <i>et al.</i> , 2019]
BFER	Representing knowledge related to building fire emergency response	[Nunavath <i>et al.</i> , 2016]
CROnto	Providing a unified and shareable knowledge base between crisis response stakeholders	[Bannour <i>et al.</i> , 2019]
EMO	Enhancing semantic interoperability of data in emergency response	[Fan & Zlatanova, 2011]
MOAC	Providing a vocabulary for crisis management	[Limbu <i>et al.</i> , 2012]
Task ontology for emergency response and planning	Representing distinct tasks related to emergency response	[Li <i>et al.</i> , 2008]
Emergency response task and data sources ontology	Representing required knowledge for geospatial data retrieval	[Wiegand & García, 2007]

We can note that in the different proposed ontologies, various aspects are represented like: studying and analysing tasks, communications, operations, organisations, resources, and many other aspects. Each one has its goals and research interest. Unfortunately, some of these ontologies are not publicly accessible, other accessible ontologies are not directly applicable in our context whereas others do not cover all of the aspects in rescue operations (Cf. Table 5.7). According to [Elmhadhbi, 2020], the aspects to cover are: persons, organisations, roles, processes, communications, incidents, time and space, and resources. Moreover, ontologies related to crisis management cannot be reused completely in our case since a rescue response differs from crisis and large-scale emergency response in many concepts. In addition, some important concepts related to our context are not well defined in previous ontologies. Furthermore, in our work, we focus

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

on modelling interactions and operations to propose an efficient communication system, so communication aspects are important. For instance, communication concepts such as the information must be linked to tasks and actors. In the literature we analyse that none of the existing ontologies considers this point. However, those ontologies can serve us to borrow ideas and some general concepts to construct our proper ontology specific for communications in French rescue operations.

3.3.2 Ontology-based approaches for designing systems and interfaces

Enhancing user interfaces with ontologies has been an interesting research area for several studies. Multiple projects with distinct purposes used ontologies on the user interface level [Paulheim & Probst, 2010]. Some studies used ontologies for information clustering as it has been done in [Fluit *et al.*, 2003; Seeling & Becks, 2003]. Other projects used ontologies for text generation [Bontcheva & Wilks, 2004; Carr *et al.*, 2001] or user interface integration [Dettborn *et al.*, 2008; Paulheim, 2009]. For this aim, multiple application ontologies were developed. However, in our best knowledge, only a few domain ontologies related to user interfaces were proposed in the literature. In this context, a domain ontology called User Interface Ontology (UIO) was proposed [Shahzad, 2011]. Unfortunately, this latter is not publicly accessible. Similarly, Paulheim & Probst [2011] proposed a domain ontology for user interfaces and interactions called UI2Ont. The authors aimed at discussing the differences between user interface (UI) description languages such as XML and a formal ontology of the domain and how both fields benefit from each other. The proposed ontology was built by extending the DOLCE and its extensions as a top-level ontology [Gangemi *et al.*, 2002]. Moreover, two core ontologies for software and software components were reused [Oberle *et al.*, 2009]. The Ui2Ont ontology consists of two levels: A top-level and a detail-level. The top-level defines the semantics of the basic terms of the domain like Interaction, Computational task, User Task, and User Interface Component. Whereas the detail-level specifies and classifies the real entities that occur in the domain like types of user interface components, like Text field and button, and user tasks that can be done with those components [Paulheim & Probst, 2011]. Moreover, research on designing systems and interfaces has evolved lately. Several studies proposed ontology-based approaches for designing systems and user interfaces. In this thesis, our main focus is on the design

of user interfaces. The design approaches can be classified into two categories. The first category includes approaches oriented to the semi-automatic generation and retrieval of personalised user interfaces based on previously defined models and ontologies. The main idea here is to present customised interfaces to the users on the basis of the defined models such as task or user models. In this context, Furtado *et al.* [2001] proposed a design method for the universal design of user interfaces where interfaces are developed for a wide community of users taking into account several differences such as preferences, habits, and cognitive style. The proposed method is based on three main levels: (1) A conceptual level where a domain expert defines an ontology containing concepts, attributes, and relations involved in the development of multiple user interfaces; (2) A logical level where a designer captures requirements of a specific user interface case and specifies several models; and (3) A physical level in which a developer derives multiple user interfaces from the previously specified models through a model-based UI generator. To this end, the authors proposed the construction of an application ontology. This latter incorporates three models like task model, user model, and domain model. Each model includes several items that can be described using different parameters with a set of possible values. Those models can be then instantiated and linked together to generate the appropriate interfaces. The proposed approach is very beneficial since it allows users to derive multiple user interfaces by taking into account different contexts and parameters. Moreover, it defines the necessary parameters to take into account in the ontology of design data type, length, and orientation, interaction way, length, number of possible values, number of values to choose, and precision together with a set of possible values for each parameter. Unfortunately, the proposed approach implies the implication of domain experts, designers, and developers in the interface design phase. Moreover, an important aspect related to the positioning of the information on the interface is not studied in this approach. Furthermore, the proposed ontology is not publicly accessible. In the same context, an ontology-based approach for user interface development was proposed based on the core UIO Ontology [Shahzad, 2011; Shahzad *et al.*, 2011]. The proposed approach consists of three levels: (1) Developing a user interface ontology by HCI experts; (2) Developing a domain ontology by domain experts; and (3) Mapping the two developed ontologies to construct a base user interface model. This model is then quantified and instantiated to develop a Graphical User Interface (GUI). To this end, at a first level, the authors proposed a user interface ontology by extending the core UIO. Hence, they defined several additional classes such as classes made

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

for data formats like textual or multimedia, or classes made for data structure such as Widget and Frames. Moreover, they defined several properties like user interaction and graphical properties that can be quantified at the GUI development process. Afterwards, they took the example of vCard as a domain ontology for a personal information management system to represent at GUI. The authors then, at a third level, mapped the two aforementioned ontologies by associating classes from both ontologies together and adding user interaction and graphical properties to the mapping. Eventually, the resultant UIM model of vCard was instantiated by using SWT (Java). Unfortunately, the UIO ontology is not publicly accessible. Furthermore, positions of information on the interface are not considered in the proposed solution, which is an important aspect in the design and generation of interfaces. The second category consists of context modelling approaches that aim at developing and retrieving user interfaces based on contextual information such as the device's capabilities and context situation. We talk here on context-aware adaptive and dynamic user interfaces. In this context, Castillejo *et al.* [2014] proposed an ontology-based solution that aims at supporting dynamic and adaptive user interfaces according to the user's context. This work was based on an application ontology called AdaptUI. The proposed ontology is composed of three main entities: User, Context, and Device. Each main entity has its characteristics such as UserCharacteristics, ContextCharacteristics, and DeviceCharacteristics. In addition, each of these classes has several sub-classes with the corresponding object and data properties. For instance, ContextCharacteristics has the sub-class Location that has hasAbsoluteLocation and hasRelativeLocation as data properties. Moreover, authors defined several necessary classes required for the dynamics and the adaptation mechanism like the class Adaptation as well as other classes like Audio, Display, and Interface. Furthermore, the authors defined several rules required for the functionality of the system. These rules were defined using the SWRL Language and divided into two different categories: Preadaptation rules and Adaptation rules. Based on these rules, the system retrieves the status of auxiliary classes to retrieve and adapt the required interface. One main drawback of the proposed solution is that user preferences are not considered. In addition, the system is based on inferences in run time using the proposed rules. This may lead to inefficiency and errors in some cases. Besides, the proposed solution does not take the type and positions of information into consideration which is an important aspect in the design of interfaces. Moreover, the proposed ontology is not downloadable nor accessible.

Furthermore, based on its description, the ontology is too specific for the proposed application. Similarly, Tsiporkova *et al.* [2012] proposed an ontology-based modelling system oriented for emergency response applications. The proposed system allows acquiring the expert and domain knowledge available within the interface design community [Tourwé *et al.*, 2011; Tsiporkova *et al.*, 2011, 2012]. The proposed system is based on a hybrid approach that combines: domain-based and context-based models. Based on these models, applications' interfaces can be retrieved and adapted. To this end, the authors proposed a three-level methodology. The first level consists in representing domain knowledge through an application ontology called HCI Core. Hence, the authors developed the ontology and defined several main classes as well as relations between them. The main classes are Activity, Application, Component, Device, Location, and Modality. This level includes obvious information such as the input/output modality supported by a component of a device. The second level lies within modelling expert knowledge related to design. Hence, the authors proposed the use of SWRL rules and added them to the proposed ontology. These rules serve as a reference for executing the required inferences in the system. Whereas, the third level is based on defining and modelling application knowledge through the instantiation of the HCI Core ontology. In this level, user interfaces are retrieved in final applications based on the context and the modelled knowledge. Unfortunately, the presented work does not consider users' preferences. Moreover, this work is limited to the selection of media components while information and their components are not considered in the design. Furthermore, the proposed application ontology is not publicly accessible.

Regardless of their category, these previous approaches share a common main drawback since they impose the implication of domain experts, designers, and developers to achieve the design and development phase, which may increase the cost and interaction problems. Alternative solutions were proposed based on the End User Development approach (EUD) [Lieberman *et al.*, 2006]. This approach is focused on a user-centred paradigm. It is defined as a collection of practices and techniques that allow final users to design and develop software objects and interfaces. In this context, Macías & Castells [2007] proposed a framework that allows final users to design their system interfaces in a customised way. The proposed framework is applied to web application authoring and consists of two systems: DESK [Macías *et al.*, 2006] and PEGASUS [Castells & Macías, 2001]. DESK is an interactive authoring tool that allows the personalisation of dynamic page-generation procedures. Whereas, PEGASUS generates HTML pages from a

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

structured domain model and an abstract presentation model [Macías & Castells, 2007]. Thanks to this framework, end users can insert new texts, remove existing tasks, replace different tasks, moving HTML objects, transforming a bullet list into a table, adding new elements to the table, and modifying text attributes such as colour and justification. To this end, the authors proposed the use of an ontology to represent domain models and users' profiles. Unfortunately, in the proposed framework, the construction of domain models is the responsibility of the end-users. These latter achieve this task by developing the ontology by themselves without any support. Moreover, the proposed framework is dedicated to individual environments and cannot be used in collaborative environments. There exist several approaches for designing user interfaces using ontologies. Multiple solutions have been developed to validate these approaches. Although each approach has its context and domain of application, none of them is complete in a way that allows end users of a collaborative communication system to design the system's and interfaces in a personalised way. Moreover, multiple ontologies for designing systems and interfaces were proposed in the literature. Table 3.2 summarises the analysed ontologies that were created to formalise knowledge related to the design of systems and interfaces. Unfortunately, some of these ontologies are not publicly accessible whereas other accessible ontologies are too specific to the proposed solutions. Those ontologies cover different aspects like user interface components, user interface properties, information properties, devices, human computer interaction, and hardware components. However, none of those ontologies covers all of the aspects at the same time (Cf. Table 5.8). Those ontologies can serve us to borrow ideas and some general concepts to construct our proper ontology specific for designing the interfaces of a communication system oriented for rescue actors.

3.3.3 Ontology-based approaches for access control and rights management

Communication systems oriented for emergency response and rescue operations are complex systems, rich in features, which are becoming more and more demanding in terms of security. It is essential to first define a security policy that is at the same time robust, efficient, flexible, fairly generic, and easy to verify. Information security is a world that brings together a set of skills. This is because the concept of information security incorporates the concepts of confidentiality, integrity, availability, non-repudiation, and authentication. One of the aspects

Table 3.2: Existing ontologies for systems and interfaces design.

Ontology	Contribution	Reference
UIO Ontology	Representing main elements for the domain of user interfaces	[Shahzad, 2011]
UI2Ont Ontology	Representing domain knowledge of user interfaces and interactions	[Paulheim & Probst, 2011]
Ontology for user interface design	Representing concepts, relationships, and attributes involved in the production of multiple user interfaces	[Furtado <i>et al.</i> , 2001]
AdaptUI Ontology	Representing knowledge for developing dynamic and adaptive user interfaces according to the user’s context	[Castillejo <i>et al.</i> , 2014]
HCI Core Ontology	Representing domain concepts and knowledge for human computer interaction	[Tsiporkova <i>et al.</i> , 2012]

of information security is Access Control (AC) which is one of its pillars. There exist several definitions of access control. Each definition depends on the domain of application and the context of use. In information security, the term “Access Control” refers to the use of mechanisms that allow authenticated entities to perform actions based on their authorisation level and to prevent entities from performing unauthorised actions [Cheaito, 2012]. There have been two simultaneous themes in the field of access control research in the past years. On the one hand, attempts are being made to create new access control models to address the security requirements of real-world applications. These have contributed to a range of successful and well-established models such as the Role-Based Access Control (RBAC) models [Sandhu *et al.*, 1996], the Team-Based Access Control (TMAC) model [Thomas, 1997], the Attribute-Based Access Control (ABAC) model [Yuan & Tong, 2005], and other models that were developed for multiple purposes [Zhou, 2008]. Around the same time, and almost independently, researchers have developed policy languages for access control [Finin *et al.*, 2008a]. These incorporate industry standards like the eXtensible Access Control Markup Language

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

(XACML) [Anderson *et al.*, 2003], but also research studies and projects, ranging from functional languages like Ponder [Damianou *et al.*, 2001] to scientific languages like the logical language [Jajodia *et al.*, 1997]. Research on access control and access rights management using semantic web technologies constitutes an interesting field for multiple researchers who have contributed and proposed several solutions in this context. These have resulted in the birth of multiple semantic web-languages and frameworks for access control policies. For instance, Kagal [2002] adopted a rule-based approach and proposed a general policy language that can be applied to agents and web services called *Rei* [Kirrane *et al.*, 2017]. *Rei* is based on deontic concepts and provides support for four different policy types: obligations, permissions, prohibitions, and dispensations [Kagal, 2002]. *Rei* was completed by the implementation of a policy engine that describes rules, defined in the policy language of *Rei*, and uses the acquired knowledge to make decisions regarding access rights and obligations [Kagal *et al.*, 2003]. Similarly, the Research Network of Excellence on Reasoning on the Web proposed Protune by adopting a rule-based approach. Protune was designed to help both the negotiation of trust and policy descriptions. To this end, several ontologies were used to define and represent concepts, the relations between them, and details of the evidence required to prove their truth [Bonatti *et al.*, 2008]. Protune provides four predicate categories to be used in rules: Decision Predicates, Logical Predicates, Constraint Predicates, Provisional Predicates. On the other hand, Finin *et al.* [2008a] used the OWL language to express Role-based access control policies. Their work follows an ontology-based approach and has led to the introduction of the ROWLBAC language and model. The proposed model includes a basic ontology composed of classic RBAC concepts, such as objects, subjects, roles, actions, and role assignments. It also includes a domain-specific ontology defined in the top of the basic ontology that includes additional attributes and relations to specify which actions are obligatory, forbidden, or permitted. The authors suggested two distinct solutions to develop the model using ontologies. The first one is based on mapping roles to values. In this case, roles are represented as a class of users, and the role dominance relation is then mapped to the subsumption relation in OWL. The second approach lies within mapping roles to classes. In this case, classes are mapped onto individuals, and users are bound to classes via the property role [Finin *et al.*, 2008b].

Research on the semantic technologies and knowledge representation was not limited to the development of access policies languages and frameworks. Multiple studies were conducted to develop and implement access control models using

ontologies. Other studies were conducted to manage access rights in real-world applications through the use of ontologies. Authors in [Cirio *et al.*, 2007] proposed a hybrid access control model that combines RBAC and ABAC models. They also proposed a supporting framework that is based on OWL-DL in which attributes are used to classify subjects into access control roles. To this end, an ontology that aimed at representing the RBAC model was proposed. This latter includes the main concepts of RBAC model such as Role, Resource, Privilege, and Action. This ontology was followed by the proposition of a domain specific ontology that captures the features of the application. The proposed two ontologies were then attached by defining relations between their concepts. Unfortunately, details on how attributes are described, allocated, related to users, or how they can be integrated with the proposed framework were not presented. Raje *et al.* [2012] worked on developing and testing a Role-Based Access Control (RBAC) framework for a solution used to assist proteomics researchers in a collaborative project community. To this end, the authors proposed an ontology that allows to determine a person's access rights based on her/his role in the departments, projects, and groups to which he belongs. The proposed ontology includes several classes and relations that ensure the representation of the RBAC model. Moreover, in order to determine the rights that a person has on a resource, the authors defined several inference rules using the SWRL language. Unfortunately, in the proposed solution, access rights are defined based on individuals of persons and not roles which is not an effective solution. Moreover, the "clear-and-reload" approach used for reasoning does not seem to be sufficient for a large system. Imran-Daud *et al.* [2016] presented an ontology-based access control framework based on a combination of ABAC and ontology technology. The proposed solution aimed at enhancing interoperability between components in a distributed environment. To this end, a generic ontology that follows the ABAC model was proposed to model different entities and their policies. This ontology models three main entities: Subject, Object, and Policy as well as the relations between them. For instance, a subject is related to an object through the relation Access Rights On. In order to apply it for different contexts, the proposed ontology can be specified and instantiated according to the domain of application. In [Imran-Daud *et al.*, 2016] the proposed solution was applied to two different scenarios: Online Social Networks and the Cloud. Buffa & Faron-Zucker [2012] proposed a rule-based approach for managing access rights in a content management system based on semantic technologies. The authors defined an application ontology called Access Management Ontology (AMO) for this aim. AMO consists of a set of classes

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

that represent different entities such as `AccessType`, `Role`, `Action`, `Agent`, `Document`, and `AuthorisedActionOnResource`. These concepts are related through a set of properties like the property `hasAccessType` that links a document to an access type and the property `hasAuthorisedAgent` that relates an agent to a document. The proposed ontology includes also a base of inference rules expressed using SPARQL queries that model the access management strategy to carry out. When added to the annotations of documents for which access should be regulated, these rules allow access to be handled according to the applied strategy. The proposed approach is innovative in that it incorporates the idea of abstraction to generalise the management of access rights in content management systems. Unfortunately, it is limited since it is restricted to the semantic web. Another ontology-based solution for access rights management and access control was proposed in [Derbale & Mehenni, 2003]. The proposed solution aimed at controlling access to shared medical records by following the Organisation Based Access Control (Or-BAC) model proposed by [Abou El Kalam *et al.*, 2003]. To achieve their objectives, the authors proposed an application ontology. This latter is composed of multiple main classes such as `Subject`, `Object`, `Action`, `Context`, `Role`, `Rules`, `Views`, and `Activities`. It also includes several object properties required to relate those classes based on the Or-Bac Model. Moreover, the authors defined several rules to define the access policy using the SWRL Language. Unfortunately, the proposed solution is based on the inference of rules during the run time which may lead to errors and inefficiency in the case of a large-scale ontology.

A large number of ontologies related to access control and access rights management were proposed in the literature. Some researchers used ontologies for representing access control models whereas others aimed at using ontologies for implementing access rights management solutions. Table 3.3 shows a summary of the analysed ontologies that were developed to formalise knowledge related to access control and rights management. Those ontologies cover different aspects like roles, organisations, actions, permissions, access rights, hierarchies, and resources. However, none of those ontologies covers all of the aspects at the same time (Cf. Table 5.9). Moreover, most of the ontologies proposed in the literature are ad-hoc ontologies developed for concrete scenarios, which restricts their generality and hinders their re-usability in different settings [Imran-Daud *et al.*, 2016]. According to [Mika, 2005], ontologies are especially helpful in formally defining the conceptualisation and inter-relationships of a domain, so that real entities such as users and data can be identified as instances of this conceptualisation. Access control and rights management can then be conveniently managed

according to the privacy-oriented interrelations specified in the ontology for the entities concerned.

3.4 Conclusions

Knowledge representation techniques and ontologies can be very helpful to design and implement an awareness and communication-support system in a way that makes it usable by fulfilling the criteria identified in Chapter 2. The main reason that lies within adopting these techniques is that they help to represent main situation's entities and then to guide the situation's perception sharing, which is an entry point to support situation awareness and interactions. Furthermore, a key first step toward designing any system oriented for a certain domain consists in capturing and representing knowledge related to the domain through relevant techniques. This will ensure to develop a system that will be accepted

Table 3.3: Existing ontologies for access control and rights management.

Ontology	Contribution	Reference
ROWLBAC Ontology	Formalising knowledge for representing RBAC security model	[Finin <i>et al.</i> , 2008a]
Ontology for modelling RBAC model	Expressing the elements of an RBAC system	[Cirio <i>et al.</i> , 2007]
Ontology for implementing RBAC mechanism	Representing knowledge for developing and testing an RBAC framework	[Raje <i>et al.</i> , 2012]
Access Control Ontology	Representing knowledge for controlling access based on ABAC model	[Imran-Daud <i>et al.</i> , 2016]
Access Management Ontology	Representing knowledge for controlling access rights to annotated resources	[Buffa & Faron-Zucker, 2012]
Ontology for implementing Or-BAC mechanism	Representing knowledge for implementing an access control mechanism based on Or-BAC	[Derbale & Mehenni, 2003]

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

by its final users and that it will be adequate with their practices. Therefore, we choose the use of ontologies as a relevant technique to represent knowledge and support the design of the system. In this chapter, we presented the principal techniques used in our research that are knowledge representation and ontologies. Hence, we started with historical background about knowledge. We then discussed the technique of knowledge representation and focused on ontologies as the selected technique for representing knowledge. In this context, we started with an overview of knowledge and representation. We then described ontologies as the selected technique for representing knowledge. Hence, we presented the definitions of ontologies, their importance, their categories, their constituents, some ontology languages, as well as the most well-known methodologies for building ontologies. Afterwards, we presented some existing ontologies related to rescue and emergency response domains and we analysed them in terms of ensuring effective communications and enhancing situation awareness. In addition, we presented several ontology-based approaches adopted for the design of systems and interfaces as well as several ontologies proposed in this context. Eventually, we moved to the literature related to access control. In this context, several ontology-based approaches developed and applied for access control and access rights management were presented with the corresponding ontologies.

As it has been shown in this chapter, several ontology-based approaches for designing user interfaces were developed. Unfortunately, none of these approaches is complete in a way that allows the end-users of a collaborative communication system to design the system's specifications and interfaces in a personalised way. In this consequence, we propose in this thesis an approach for identifying the system's specifications and designing its interfaces by its end-users. The proposed approach includes the integration of an access control policy to guarantee the confidential access to information in the system to develop. To this end, a platform that allows the design of the system interfaces and specifications in a customised way is proposed. This approach consists of a five-step methodology. The first step consists in examining and modelling interactions based on real practices. The importance of this step is to identify the information required by each person based on her/his role, context, and tasks to achieve. The second step lies within the construction of an application ontology that represents the knowledge required for designing a communication and awareness-support system oriented for rescue actors that guarantees the confidentiality of information. This ontology consists of three modules. The first module is oriented for representing knowledge related to communications in rescue operations. It serves for ensuring

a common interpretation of information between different stakeholders as well as representing and formalising different procedures and flow of information. The second module incorporates knowledge required for the dynamic design and configuration of the system and interfaces. Whereas, the third module is specific for guaranteeing access control management in the system. In order to manipulate the processing of different inferences, it is important to define relations between different concepts and instances based on real interactions. Hence, the first and the second steps are interdependent between them. The third step consists in developing MODES, an ontology-based platform for design and communication. Based on the previously developed ontology, this platform will allow the end-users of the system to define its specifications and design its interfaces in a customised way and to communicate efficiently in rescue operations. The importance of using an ontology in this step is to develop a flexible platform that allows the dynamic configuration of the system. Regarding the fourth step, it consists of guaranteeing confidential access to information through access control and rights management mechanisms. Hence, we propose an ontology-based access control policy to reinforce information confidentiality. Whereas, the fifth step consists in designing the system's specifications and interfaces by its end-users in a customised through the proposed platform. The aim of passing through these steps is to propose a usable, and flexible system that guarantees the confidentiality of information and can be accepted by the stakeholders.

3. KNOWLEDGE REPRESENTATION AND ONTOLOGIES

Chapter 4

Modelling Interactions

Contents

4.1	Introduction	90
4.2	Rescue Operations in French Context	91
4.2.1	Involved organisations and actors	91
4.2.2	Organisational Model	94
4.2.3	Scenario of a rescue operation	96
4.3	Modelling Interactions and Communications	99
4.3.1	Requirements for modelling interactions	99
4.3.2	Rescue operation chronology	101
4.3.3	Structural model	103
4.3.4	Interaction model	105
4.4	Conclusions	118

4.1 Introduction

This research project aims at supporting the design of an information sharing and communication system for daily rescue operations in France. The proposed system aims at resolving interaction problems and ensuring effective communications, which will surely help to enhance situation awareness amongst rescue actors. As it has been mentioned in Chapter 3, we propose in this thesis an approach for designing a communication system that aims at supporting situation awareness in rescue operations. The proposed approach follows a five-step methodology illustrated in Figure 1.1. As we can see in Figure 1.1, the first step in the proposed approach consists in analysing and modelling communications and interactions in these operations through the study of documents, reports, and legislation related to the domain. This study allows us to identify different services as well as their missions, to analyse procedures, and to link these missions with interactions. Moreover, this study leads to identifying the requirements, criteria, and actionable information for actors on the basis of operational practices. Furthermore, it helps to represent those procedures and interactions in a formalised way. Giere [2004] defines models as a representation of reality. However, before analysing and modelling any activity or procedure, it is fundamental to identify actors and services that are involved in these activities. Moreover, this process of comprehensive identification is also the basis for modelling communications since it identifies different entities that handle these communications and interactions. We notice that, in this work, our study is limited to daily rescue operations. To this end, we examine interactions, communications, and activities in those operations. However, the work done does not cover large-scale and disaster response. In the French case, several documents that describe the rescue response procedure were elaborated by the state. However, there is no specific plans that are applied in this case. Some plans were elaborated and can be activated such as ORSEC, the NOVI plan, and the white plan [Elmhadhbi, 2020]. However, the application of those plans is specific to particular cases and is not related to daily rescue operations. The plan ORSEC provides the general framework of the response process in large-scale events such as disasters. The NOVI is the reference plan for the on-site mass causality management. Regarding the white plan, it is used to identify a set of hospitals where the victims can be transported in case of large-scale events that cause a large number of victims. The activation of those plans require the involvement of additional actors such as mayors and prefects who are not involved in daily rescue operations. In this chapter, we introduce

4.2 Rescue Operations in French Context

first organisations and services involved in French rescue operations as well as their missions. Moreover, we present an organisational model. This model shows the different organisational levels as well as a general flow of information and decisions between different levels. We then describe a scenario of a rescue operation derived from practices applied in France. This scenario will serve as a basis for our study. It is described based on a study of domain-related documentation such as reports as well as previous studies. Afterwards, we identify the required elements and parameters to be taken into account when modelling interactions in complex contexts such as rescue operations. Moreover, we present the main phases of a rescue operation. Furthermore, we propose a structural model based on those requirements. Eventually, we propose an interaction model that shows interactions between different actors in French rescue operations.

4.2 Rescue Operations in French Context

In France, the rescue of people is defined as specific tasks to be accomplished by public services in order to ensure the safety of patients and victims by making them able to escape from dangers, securing intervention sites, providing medical help, and finally, ensuring the evacuation to an appropriate place of reception [Cazeneuve & Touraine, 2015]. Two main services are responsible for the rescue and emergency response operations: Firefighters and emergency medical services. Several private associations such as non-governmental organisations also participate in rescue and emergency response operations. However, their participation is limited to operations and response in case of large-scale events where firefighters and medical services require support and reinforcements. In this section, we provide a discussion about missions as well as the composition of French firefighters and emergency medical services. We then present a model that shows organisational levels in French rescue operations. Eventually, we describe a scenario of a rescue operation derived from French practices. The reason behind focusing on analysing activities and interactions of French organisations is that the system we aim to develop is oriented toward supporting French stakeholders.

4.2.1 Involved organisations and actors

A detailed referential has been published by the French state to clarify the missions and responsibilities of public services involved in rescue operations and urgent medical help [La DDSC et la DHOS, 2009; Richard-Hibon & Braun, 2009].

4. MODELLING INTERACTIONS

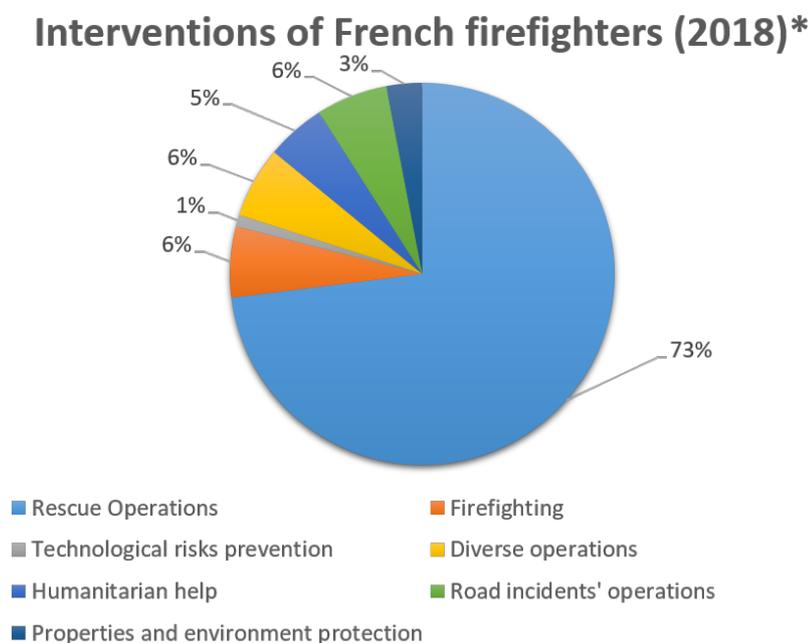


Figure 4.1: Distribution of operational activity by categories.

*Percentages are extracted from [French Ministry of Interior, 2019].

Moreover, a detailed description of the organisation and hierarchy of each service is presented in this referential.

Firefighters: known as Local Services for Fire and Rescue (SDIS), firefighters are responsible for firefighting, preventing and evaluating risks, preparing rescue measures and organising emergency resources, protecting places and environment, providing humanitarian help, and rescuing persons in distress situations such as victims of incidents. A recent study shows that interventions related to rescue operations remain the principal activity of French firefighters as shown in Figure 4.1. Figure 4.1 shows the distribution of the operational activity of French firefighters by intervention categories in 2018. On a total of 4942932 interventions performed by French firefighters in 2018, 73% of interventions were oriented for rescue operations while only 6% were dedicated to firefighting [French Ministry of Interior, 2019]. SDIS are departmental services which means that each French department has his SDIS composed of professional firefighters, volunteers, administrative and technical staff. Furthermore, each SDIS is composed of several centres and services that manage distinct tasks and duties. as presented in Figure 4.2. Figure 4.2 illustrates different services and centres that compose a

4.2 Rescue Operations in French Context

SDIS. It also shows the composition of those centres and services. As we can see in Figure 4.2, a SDIS disposes of one or several Call Processing Centres (CTA) composed of CTA Operators that receive and process alerts, choose materials and persons to engage with respect to the nature of calls, manage resources, and ensure communication with other services and centres. Moreover, each SDIS possesses several Fire and Rescue Centres (CIS) composed of rescuers and CIS Operators responsible for engaging and sending resources chosen by the CTA to the intervention sites, communicating with intervention teams, and sending reinforcements if necessary. In addition, every SDIS has a Departmental Emergency Operations Center (CODIS) that is responsible for coordinating the activity of different centres. Besides, each SDIS possesses a Health and Medical Rescue Service (SSSM) that is composed of firefighter nurses and doctors. SSSM is responsible for monitoring the physical condition of firefighters, preventive medicine counselling, and providing medical care for firefighters. SSSM also contributes to emergency rescue missions relating to providing urgent medical aid and ensuring medical transport in critical situations.

Emergency Medical Services: They are also known as Urgent Medical Assistance Services (SAMU). SAMU are hospital services whose main mission consists in providing medical help for victims in distress situations outside hospitalisation centres. Moreover, they are involved in rescue operations by providing medical instructions to firefighters present at intervention sites. Similarly to SDIS, each SAMU possesses several centres and services that manage distinct tasks and duties as presented in Figure 4.3. Figure 4.3 illustrates different services and centres that compose a SAMU. It also shows the composition of those centres and services. As it is shown in Figure 4.3, each SAMU has several Call Reception and Dispatch Centres (CRRA) that are composed of operators and medical regulators. Their responsibility consists in providing medical listening and regulation, choosing adequate responses with respect to the nature of calls, checking the availability of

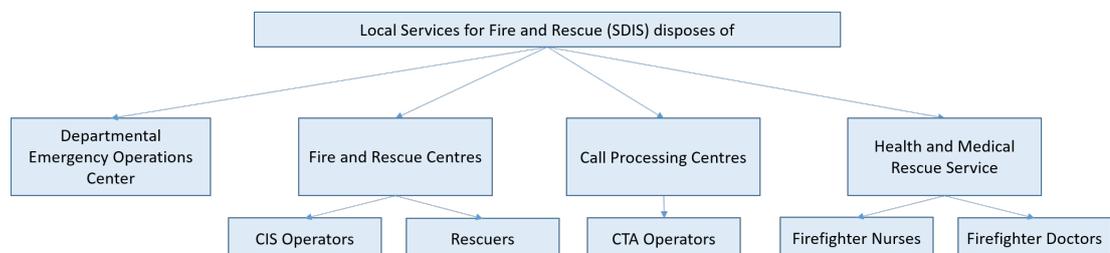


Figure 4.2: Composition of a SDIS: Centres and services.

4. MODELLING INTERACTIONS

hospitalisation centres, preparing the transportation and evacuation of victims using health transport organisations if required and, ensuring victims' admission in hospitalisation centres. Those CRRAs are interconnected with CTAs of SDIS to optimise the response provided by the rescue and emergency care chain. In addition, each SAMU is connected to another hospitalisation service so-called Mobile Service of Emergency and Reanimation (SMUR) that provides care for patients or victims whose conditions require, urgently, medical care and resuscitation. SMUR teams are solicited based on SAMU requests. They are generally composed of a doctor specialising in emergency medicine and a nurse.

4.2.2 Organisational Model

Effective emergency response and rescue operations require pre-established response structures as well as a predefined reliable chain of command [Labba *et al.*, 2017]. Moreover, in order to achieve successful operations, the different involved services and centres have to cooperate and communicate to accomplish their missions and duties on multiple organisational levels. In this context, the multidisciplinary services and centres involved in French rescue operations are scattered on different decision levels as shown in the organisational model in Figure 4.4. Figure 4.4 shows a model that represents the organisational levels in French rescue operations, the composition of each level, and the general flow of decisions and information between these levels and within each level. As we can see in Figure 4.4, in the French context, the hierarchical chain of command is composed of three main levels: The strategical level, the tactical level, and the operational level [Labba *et al.*, 2017; Saoutal *et al.*, 2014].

Strategical level: This level consists of public authorities' members as well as

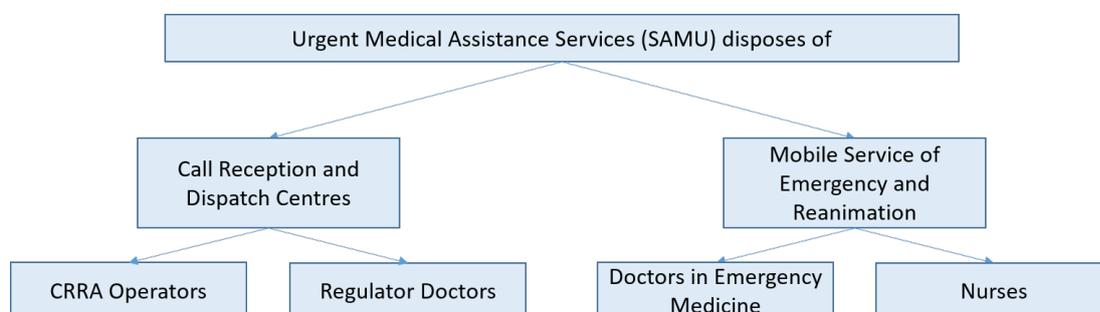


Figure 4.3: Composition of a SAMU: Centres and services.

4.2 Rescue Operations in French Context

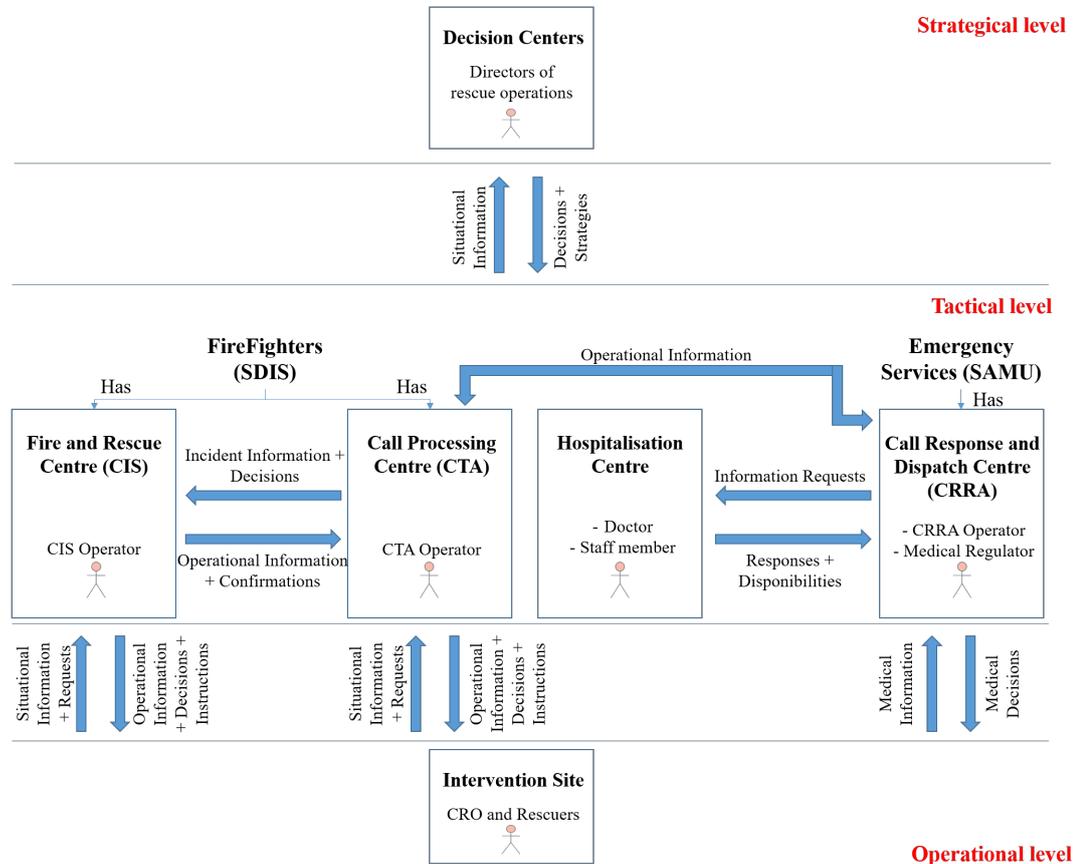


Figure 4.4: Hierarchical tree of command and general flow of information and decisions.

representatives of the various services with different responsibilities and cultures that play the role of directors of rescue operations. Their main mission consists in fixing the strategy of the response. To this end, actors at this level take major decisions together and deploy the measures taken according to situational information received from the field through the tactical level. Those decisions and strategies are then communicated to the tactical level.

Tactical level: This level is composed of the command and control of each emergency response organisation in addition to involved actors in hospitalisation centres. It consists of doctors and staff members in hospitalisation centres as well as operators and regulators in operational centres represented by CTA operators in Call Processing Centres (CTA) of Firefighters (SDIS); CIS operators in Fire and Rescue Centres (CIS) of Firefighters (SDIS); And CRRA operators

4. MODELLING INTERACTIONS

and medical regulators in Call Response and Dispatch Centres (CRRA) of Emergency Medical Services (SAMU). Their role is to fix the operational plan such as resource allocation, task priority. To this end, services and centres within this level exchange operational information as well as information on incidents and availabilities. They are also responsible for ensuring the communication between stakeholders, and between the strategic and the operational levels in case of need. Moreover, a principal mission of actors at the tactical lies within orienting rescuers in the intervention sites by giving instructions based on situational information.

Operational level: This level consists of different agents in the intervention site represented by a Commander of Rescue Operations (CRO) and other rescuers. Their main mission is to execute the operational plans on site. In order to maintain a common operational picture and to receive relevant instructions, actors at the operational level communicate with appropriate actors at the tactical level. For instance, situational information is transmitted from the intervention site to the Fire and Rescue Centres (CIS) and the Call Processing Centre (CTA). On the way back, corresponding decisions and instructions are transmitted from those centres to the rescuers at the intervention site.

In the case of small-scale rescue operations, which are the main interest of our work, most of the operations and communications take place at two levels only: The tactical and operational level. Whereas, the implication of the strategical level is limited to large-scale operations such as crisis management and large events emergency responses. Hence, we have focused our work on analysing and modelling communications and interactions between the tactical and operational levels.

After having identified organisations and actors that are involved in French rescue operations, it is important to analyse their tasks and interactions in a scenario of operation. This will help to understand the tasks of each actor depending on her/his role. Moreover, this identification constitutes a first step toward analysing and modelling interactions and practices. In the next subsection, we present an example of a rescue operation scenario. This scenario will constitute a departure point for our research study. It was defined based on a study of documents, existing reports, and legislation related to the domain.

4.2.3 Scenario of a rescue operation

Derived from French practices, this scenario represents a medical rescue operation case after an accident causing one or several casualties as shown in Figure 4.5.

4.2 Rescue Operations in French Context

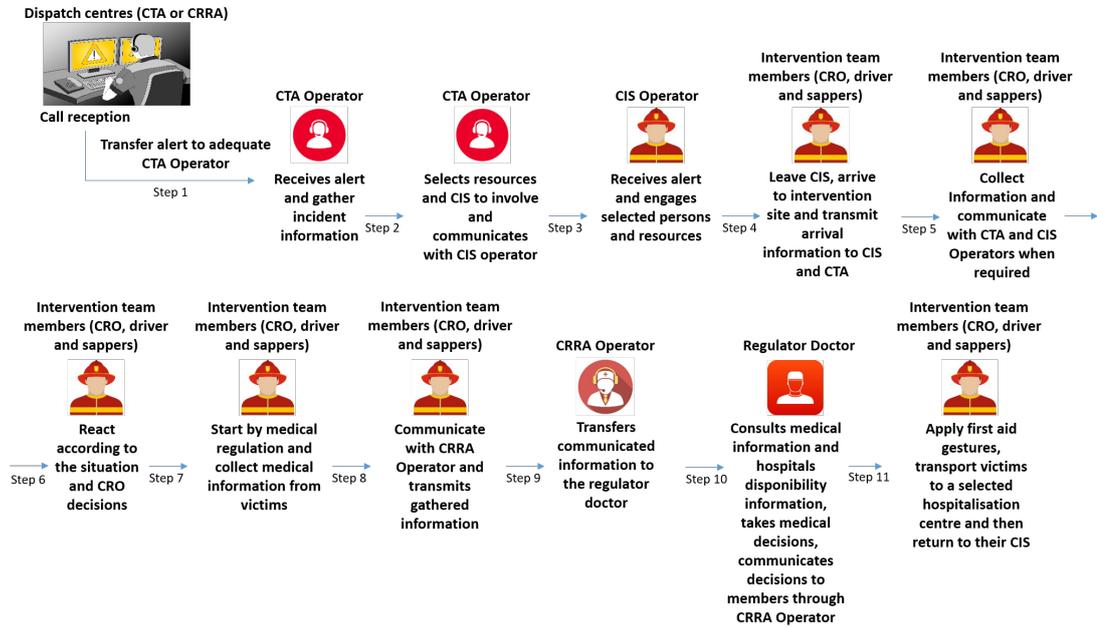


Figure 4.5: Process of a medical rescue operation.

Figure 4.5 illustrates the process and main steps in the described scenario. As we can see in this figure, when an incident occurs, eyewitnesses or victims may call the involved services by themselves to communicate about the incident and ask for help. In France, two phone numbers are dedicated to this purpose. The first number is “18” which is the number of firefighters and puts the caller in direct relation with a CTA operator. Whereas the second number is “15”. This is the number of CRRA of medical services and puts callers in relation with a CRRA operator who transmits the calls to a CTA operator when the intervention of firefighters is required. Regardless of the dialled number, the CTA operator receives an alert through a direct call from victims or eyewitnesses or an indirect call transferred by a CRRA operator. Hence, the CTA operator starts by retrieving information about the incident, the intervention site, and availability. Accordingly, the CTA operator selects a CIS to involve as well as the required persons and material to engage. The CTA operator communicates then this information to the operator of the selected CIS through a departure ticket. Hence, The CIS operator receives the departure ticket and confirms its reception to the CTA operator. Once done, the CIS operator engages the selected team, which is generally composed of a driver, a CRO, and multiple sappers. In case of any technical problem or the engagement of another material or person, the CTA operator is informed by the

4. MODELLING INTERACTIONS

CIS operator through a problem and engaged resources report. Otherwise, the selected team prepares for departure and leaves the CIS toward the intervention site with the chosen vehicles and materials. Hence, the driver drives the selected vehicle while the CRO and other members represented by sappers prepare for intervention through studying the available information and consulting the intervention plans. Afterwards, the intervention team arrives at the intervention site and the CRO transmits the arrival information to the CIS and CTA operators. Hence, team members access the intervention site and collect information in order to assess the initial state of the situation. In the case of any problem or the need for reinforcement, the CRO fulfils a situation report and sends it to CTA and CIS operators who act according to the CRO report. Otherwise, the CRO does not make any report about the initial situation. After having collected the initial situation information, The CRO makes decisions based on the situation and assigns tasks to other members. Thus, the team members execute tasks and carry actions based on situation evolution, decisions taken as well as the role and function of each one. When safety, protection, and information gathering tasks are completed, the team members move to the second part of the operation which consists in regulating and evacuating victims. Therefore, those members start by collecting detailed information on the condition of the victims. Collected information is then communicated by the rescuers to the CRRA operator who transmits it to the regulator doctor. Based on the medical information related to victims as well as information related to the availability of hospitals, the regulator doctor takes her/his decisions and communicates these decisions to the CRRA operator who transmits them to the CRO and other team members. On the basis of communicated decisions, rescuers apply first aid gestures to the victims. Afterwards, rescuers prepare the transportation of victims and leave then intervention site toward a relevant hospitalisation centre selected by the regulator doctor. The CRO informs CTA and CIS operators of departure information as well as information related to the final situation. On the way toward the hospital, and while the driver drives toward the hospitalisation centre, the CRO and other members monitor the victim and communicate with the CRRA in case of need. Rescuers arrive then at the hospitalisation centre and there is a reception of the victims. Later on, the team members leave the hospitalisation centre and return to their CIS. Once arrived in the CIS, information about the arrival is transmitted to the CIS and CTA operators by the CRO in order to update the availability of team members and vehicles. Eventually, rescuers arrive in CIS, the CRO fulfils an intervention report and the intervention arrives at its end.

In this subsection, we described a scenario of a rescue operation derived from French practices. This scenario constitutes a basis for analysing and modelling practices and interactions. It was defined based on existing reports and documents related to the domain. Although the proposed scenario is limited to rescue operations in France, this latter is characterised by its generality since it is not limited to a specific kind of accident.

4.3 Modelling Interactions and Communications

After having identified participating services in rescue operations, their missions and their activities, as well as presenting an organisational model, let us move to the interactions modelling phase. As a first step, one needs to identify modelling requirements and model components. Therefore, we request several requirements for modelling interactions. Moreover, we propose a structural model based on those requirements. In addition, we present the main phases of a rescue operations. Eventually, we provide an interaction model on the basis of the scenario described in [4.2.3](#).

4.3.1 Requirements for modelling interactions

The principal purpose of our model is to represent interactions and information flow in rescue operations and then to provide a solution that aims at enhancing situation awareness. Models are generally defined as clear and explicit representations of some portions of reality as perceived by some actor [Wegner & Goldin, 1999]. Modelling is essential in supporting complex human design activities. In the development of information systems, as well as the re-engineering of work practices, the modelling of processes or workflows often plays a central part [Krogstie *et al.*, 2006]. Related to awareness, reaching its highest level requires perceiving all factors of a situation within a volume of space and time as well as understanding their senses and relations. Furthermore, it is fundamental to determine each and every relevant information that informs on a situation as a first step toward supporting communications. Therefore, identifying situation elements and relevant information is the first step heading to improve situational awareness. These are the essential elements to take into account when modelling processes and interactions. The first element to take into account is *Actors*, their

4. MODELLING INTERACTIONS

Roles, and their *Positions* in the organisational levels of operations. Any rescue operation requires the engagement of many persons who can play distinct roles according to their functions, skills, and position at the organisational levels. Therefore, making the difference between various actors, roles, and organisational levels of operations is important for modelling. The second element to consider is the tasks and actions executed. Every actor has to accomplish different actions in order to fulfil her/his responsibilities. Some actions are the responsibility of single actors and may produce or require situation related information while other actions need the interaction and collaboration of multiple actors and generate an information flow between them. Hence, it is also important to consider them since most of the interactions are based on these actions. In our model, we refer to actions and activities by *Tasks*. Another primary element is *Information*. This is the foundation of interactions and situation awareness. It instructs on situations and all the perceived elements in an environment. In this context, specifying which group of information and corresponding information is being shared or consulted at each step is vital in modelling interactions. In addition, exchanging and consulting this information require using appropriate communication tools. Consequently, it is also crucial to identify the *Instrument* that enables communication together with the type of communication. Furthermore, actors involved in rescue operations are geographically separated. Some of them are present in intervention sites like first responders, while others stay in dispatch or rescue centres. As already explained, operations, tasks, and communications take place at different locations. It is thereby required to distinguish between distinct *Locations* when modelling. Finally, it is of the highest importance to consider the *Time* parameter since rescue operations are dynamic and evolve continuously with time evolution. This dynamic aspect alters the state of other situation elements such as tasks and situation information. Thus, two dimensions must be considered : Time and Locations. From all of the above, we can summarise elements to take into account when modelling interactions by

- *Actors*, their *Roles*, and their *Positions* in the organisational levels of operations
- *Information*
- *Communication instrument*
- *Tasks*

4.3 Modelling Interactions and Communications

- *Time*
- *Location.*

However, modelling complex processes, such as rescue operations, while taking into account the time parameter is explicitly challenging. Nunavath & Prinz [2015] state that modelling complex and dynamic activities requires splitting those processes into many phases and separating them with respect to time. Therefore, we split a rescue operation into several main phases including each many sub-phases. In the next subsection, we present different phases and sub-phases of a rescue operation and we illustrate their chronology on a timeline.

4.3.2 Rescue operation chronology

As being mentioned in the previous subsection, we split a rescue operation into multiple phases and sub-phases to facilitate the modelling process. Moreover, we precise multiple time instances that separate different sub-phases. Figure 4.6 illustrates the chronology of phases and sub-phases in a rescue operation. As we can see in Figure 4.6, a rescue operation can be split into six principal phases. The first phase of a rescue operation is Alert that has a single sub-phase: Alert Processing and Reception. During this phase, the alert is received and processed in CTA. The first information about the incident is collected to select adequate resources. Moreover, this information is transmitted to CIS to engage selected resources. After the Alert phase, comes the phase entitled Involvement of required

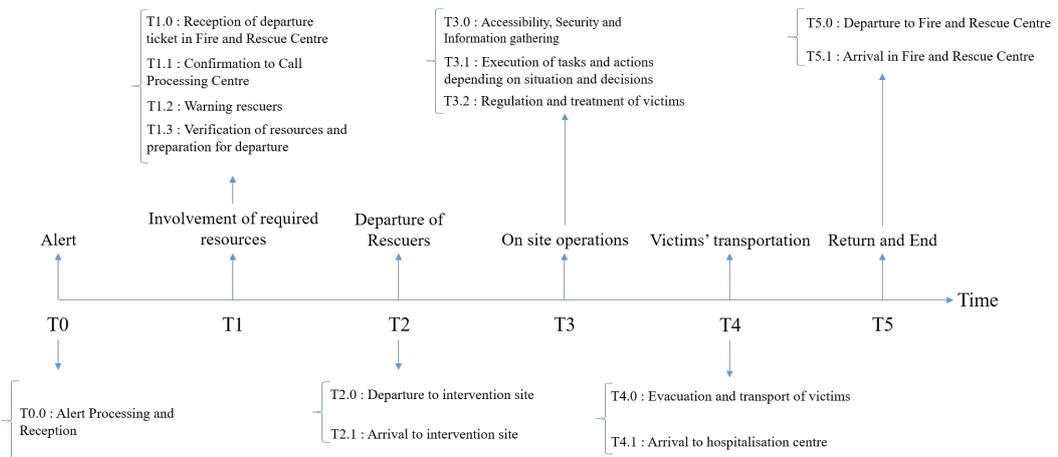


Figure 4.6: Chronology of phases and sub-phases in rescue operations.

4. MODELLING INTERACTIONS

resources. This latter has four sub-phases respectively: Reception of departure ticket in fire and rescue centre, Confirmation to call processing centre, Warning rescuers, Verification of resources, and preparation for departure. This phase includes the reception of communicated information in the CIS as well as the confirmation of reception of this information. Moreover, it incorporates the engagement of the resources selected during the first phase. Regarding the third phase, it consists of the departure of rescuers. The aforementioned phase has two sub-phases represented by the departure and arrival to the intervention site. During this phase, rescuers depart with the selected vehicles and material to the incident site. This phase also includes the communication of departure and arrival information with CTA and CIS Operators. After the arrival to the intervention site, a new phase begins. Called On-site operations, this phase has three sub-phases. The first sub-phase is Accessibility, Security, and Information gathering. This sub-phase is followed by another one that consists of the Execution of tasks and actions depending on the situation and decisions. Whereas the third sub-phase is the Regulation and treatment of victims. The above-mentioned phase includes the achievement of adequate actions on the intervention site on the basis of the actual situation. Those actions include protecting victims, ensuring the security of intervention site, collecting situational and medical information, and providing first aids to victims. Moreover, the mentioned phase consists in selecting an adequate hospitalisation centre to receive victims. Afterwards, comes the phase entitled Victims' transportation. This latter has two sub-phases. The first sub-phase consists of the Evacuation and transport of victims. Whereas, the second sub-phase is represented by the arrival of rescuers to the hospitalisation centre. This phase consists of the departure of rescuers from the intervention site toward the hospitalisation centre selected in the fourth phase. It also consists in monitoring the victims' status till the arrival to the hospitalisation centre and reception of victims in this latter. Information about departure and arrival to hospitalisation centre is communicated during this phase with CIS and CTA operators. When victims are received in the hospitalisation centre, the intervention arrives at its end and the last phase begins. This latter is referred to as Return and end. It includes two sub-phases. The first sub-phase is the departure of rescuers to Fire and Rescue Centre while the second sub-phase is represented by the arrival in the Fire and Rescue Centre. The aforementioned phase consists of the return of rescuers to their appropriate centres. It also incorporates the fulfilment and archiving of the final intervention report. After having identified the main elements to consider in modelling interactions and presenting the chronology of

phases in rescue operations, we move now to presenting a structural model. This latter includes all the necessary defined parameters to take into consideration for modelling interactions.

4.3.3 Structural model

There exist several approaches and techniques to represent and formalise processes, activities, and interactions. Some techniques are based on business process models and diagrams while others are derived from multi-agent approaches. In this thesis, we choose to adopt the approach that is based on business process modelling by extending UML diagrams due to many reasons. The first reason is that process models and diagrams can be used to model dynamic processes, interactions, and sequences by taking several parameters into consideration. The second reason is that business process models enable the representation of information flow between different actors, which is important for modelling interactions. Eventually, the third reason is that UML Diagrams are precise, and intended to describe specifications of an information system, which is responds to our needs since our objective is to design an operational communication system. However, none of the existing UML diagrams allow representing interactions in a single model by taking into consideration all the previously defined parameters. To this end, we do a mixture of UML Collaboration Diagram, UML Activity Diagram, and UML Sequence Diagram [Glasse, 2008] to represent our model clearly in one diagram as shown in the illustrative example in Figure 4.7. The Sequence diagrams are mainly used to represent the time order of a process. They describe interactions between actors' roles along a temporal line and allow the representation and illustration of the sequential size of each step. The activity diagrams allow the representation the flow of activities from one activity to another activity and thus they serve to show the flow of tasks. This flow can be sequential, branched or concurrent. Regarding the collaboration diagrams, they serve for the representing the structural organisation and the messages that are sent and received. The collaboration diagrams are similar to the sequence diagrams. The main distinction between them is that the collaboration diagram arranged elements according to space, the sequence diagram is according to time. Eventually, business process models serves for modelling processes and interactions while taking into account additional parameters such as the organisations and hierarchical levels, as well as the communication devices. In Figure 4.7, the

4. MODELLING INTERACTIONS

proposed structural model is based on two axes, a vertical one representing time and a horizontal one representing locations.

- **Time axis:** Allows the visualisation of the sequence of activities and actions with respect to time. Moreover, it allows the separation between different phases and sub-phases of an operation. These sub-phases are separated vertically through different timestamps.
- **Location axis:** Allows the separation between different places in which an action occurs or information is being shared or consulted. To this end, locations are separated horizontally through different columns.

Furthermore, this model includes actors and their roles together with their position in the organisational levels of operations represented by an icon of a dummy person. This actor can execute a task represented by rectangles with rounded corners. To do that, s/he needs access to some information. In addition, any task can generate information to be exchanged with other actors. Information is represented by rectangles in the model. Moreover, the proposed model also includes the communication device used to exchange or visualise information. Indeed, three types of devices are used in rescue operations so that information is transmitted and received through three possible ways: Non-oral communication via Mobile phones represented by green mobile phone icons; Non-oral communication via desktops represented by blue desktop icons; And oral communication through

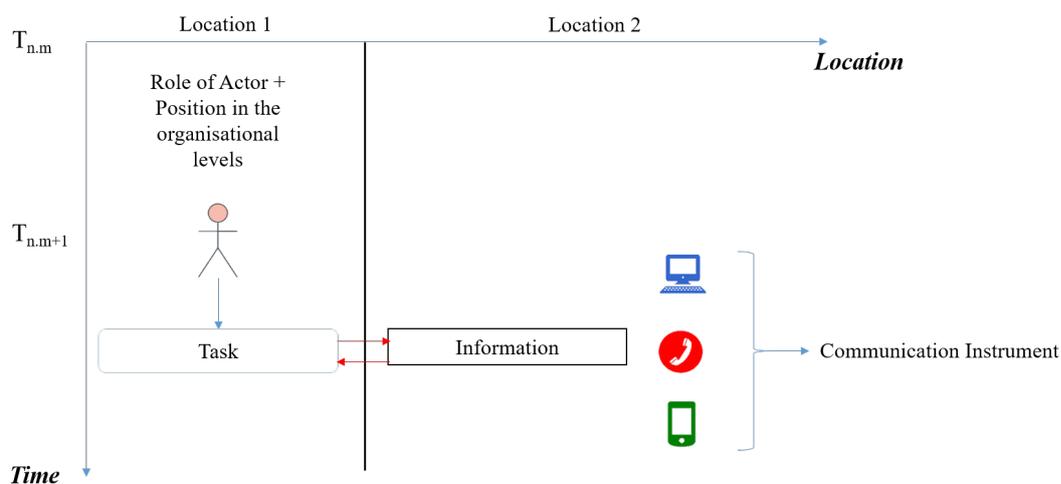


Figure 4.7: Interactions structure model.

4.3 Modelling Interactions and Communications

radio devices and handsets represented by red circle icons. We notice that the proposed structure model aims only at representing the main parameters to take into consideration when modelling interactions. In addition, it is a general model that serves as a reference to illustrate the interactions through an interaction model and does not represent any specific case in rescue operations where several activities may run in parallel. After creating the structure model, we move to the last step, which is building up an interaction model for rescue operations. In the next subsection, we present the proposed interaction model.

4.3.4 Interaction model

In order to construct the proposed interaction model, we adopt an approach based on French procedures and practices. To this end, we take the rescue operation scenario described in 4.2.3 as a reference for modelling interactions and practices. The aforementioned scenario is characterised by its generality since it is not limited to a specific type of accident. It was described based on a deep study of domain-related documentation. Moreover, we take the structure model presented in 4.3.3 as a basis for illustrating the interaction model. In addition, in the interaction model, we consider the totality of the elements required for modelling interactions. Furthermore, to model interactions and practices in a clear and simple way, we follow the chronology of rescue operations described in 4.3.2. The proposed interaction model is presented in figures 4.8 to 4.20. We notice that in those figures blue arrows represent the sequence of tasks. Red arrows are used to show the relation between the tasks and the produced or required information if any. While black arrows are used to show the information flow between actors and thus between the organisational levels of operations. Moreover, in those figures, we highlight tasks that need the interaction and collaboration of multiple actors by underlining them. In addition, we separate between different sub-phases of a given phase by indicating time instances and changing the background colours. Eventually, for simplicity of modelling and interpretation, we classify the information elements into groups that are produced or used by tasks. When an incident occurs, eyewitnesses or victims may call the involved services by themselves to communicate about the incident and ask for help. The CTA operator who exists in the CTA receives an alert at the tactical level. When an alert is received, the first phase entitled Alert phase begins at T0.0 as shown in Figure 4.8. Figure 4.8 represents actions, communications, and interactions during the alert phase. As we can see in Figure 4.8, the CTA operator starts by retriev-

4. MODELLING INTERACTIONS

ing information about the incident, general information about the intervention site, general information about victims, and information about specific dangers. Following this retrieval, the CTA operator fulfils the collected information into the system through a desktop computer. This task produces five groups of information containing each multiple information elements as illustrated in Figure 4.8. For instance, incident information contains the type, address, time, and date of the incident. Moreover, the CTA operator consults cartography information to select and engage appropriate resources. Hence, s/he consults three groups of information where each group has multiple information elements. The groups that are required for this task are centres', materials', and persons' cartography. On the basis of the consulted information, the CTA operator selects a CIS to involve as well as the required actors and material to engage. This task produces three groups of information that are centre to engage, material to engage, and actor to involve. The CTA operator communicates then these information to the operator of the selected CIS through a departure ticket. This latter contains the totality of the collected information as well as information about material, actors to engage, and accessibility information related to the intervention site. Steps 1, 2, 3, 4, and 5 in Figure 4.8 represent these tasks respectively. When the departure ticket is transmitted by the CTA operator, the alert phase arrives at its end and a

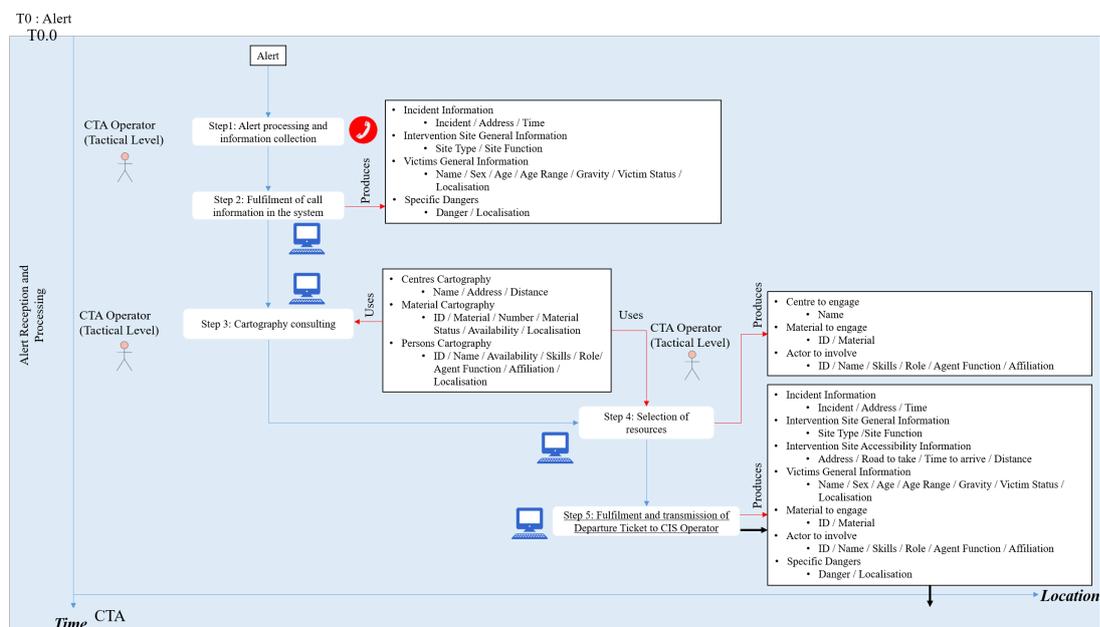


Figure 4.8: Interactions during the alert phase.

4.3 Modelling Interactions and Communications

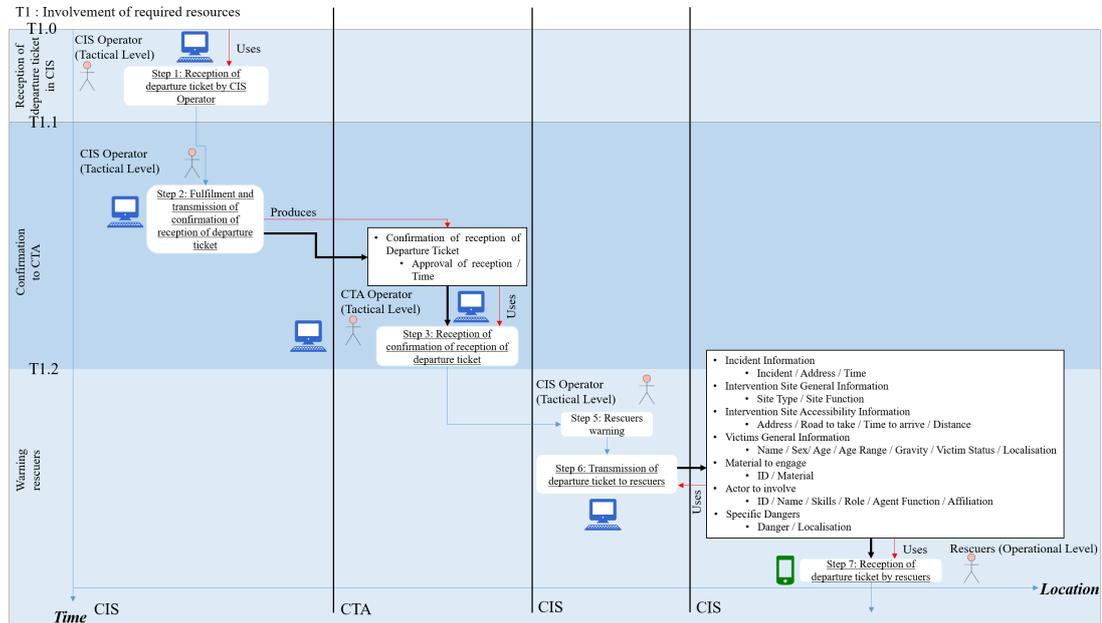


Figure 4.9: Interactions during the involvement of required resources (1).

new phase begins. This latter is entitled Involvement of required resources. Figures 4.9 and 4.10 show interactions during the involvement of required resources phase. As we can see in Figure 4.9, the involvement of required resources starts at T1.0 with the reception of departure ticket by the CIS operator in the CIS through a desktop computer. When the departure ticket is received, the CIS operator confirms to the CTA this reception at T1.1 during the sub-phase entitled Confirmation to CTA. To this end, the CIS operator fulfils a confirmation of reception of departure ticket and communicates it with the CTA operator who receives this confirmation in the CTA. The confirmation report includes approval of reception as well as the time of reception. These tasks are represented in steps 1, 2, and 3 in Figure 4.9. At T1.2, a new sub-phase that consists in warning rescuers begins. During this sub-phase, the CIS operator engages the selected team, which is generally composed of a driver, a CRO, and multiple sappers. To this end, the CIS operator transmits the departure ticket to the rescuers who will receive this ticket using mobile devices in the CIS at the operational level. Steps 5 and 6 in Figure 4.9 represent these tasks respectively. Following the reception of departure ticket by rescuers, a new sub-phase entitled Verification of resources and preparation for departure starts at T1.3. During this sub-phase, rescuers start with checking selected material and preparing for departure. Steps 1 and

4. MODELLING INTERACTIONS

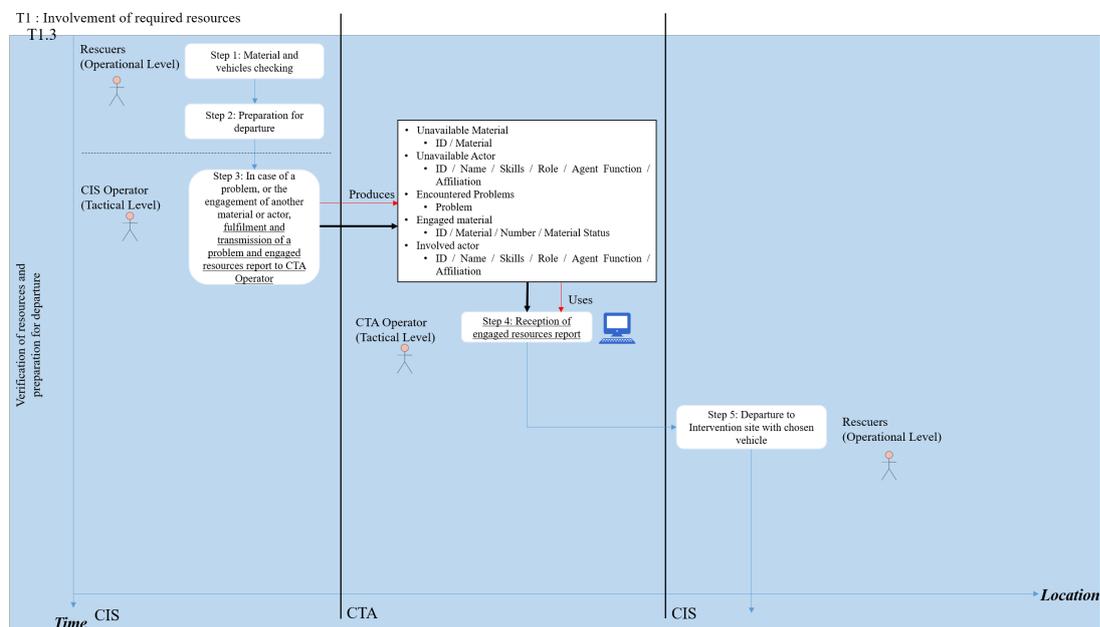


Figure 4.10: Interactions during the involvement of required resources (2).

2 in Figure 4.10 represent these two tasks respectively. In case of any technical problem or the engagement of another material or person, the CIS operator fulfils a problem and engaged resources report and transmits it to the CTA operator. The aforementioned report includes information about unavailable material or actor, encountered problems if any, engaged material, and involved actor. In this case, the CTA operator receives the transmitted report in the CTA. These two tasks are represented by steps 3 and 4 in Figure 4.10. Otherwise, the selected team leaves the CIS toward the intervention site with the chosen vehicles and materials. Step 5 in Figure 4.10 represents this task. Following this task, a new phase called departure of rescuers starts at T2.0 with the sub-phase entitled Departure to intervention site. Figures 4.11 and 4.12 represent interactions during the departure of rescuers phase. At the beginning of this sub-phase, using a mobile device, the CRO fulfils information about the departure and transmits it to CIS and CTA operators who exist in CIS and CTA respectively at the tactical level. The transmitted information includes departure from CIS information, engaged material, and involved actor. It is then received and consulted by the aforementioned operators. These tasks are represented by steps 1 and 2 in Figure 4.11. Afterwards, the rescuers head towards the intervention site. Hence, the driver drives the selected vehicle. For this aim, he consults information about

4.3 Modelling Interactions and Communications

intervention site accessibility such as address, road to take, time to arrive, and distance. Whereas, the CRO and other members represented by sappers prepare for intervention through studying the available information and consulting the intervention plans. In this context, they have to consult intervention site general information, general information about the victims, as well as information related to water resources and specific dangers. Steps 3, 4, and 5 in Figure 4.11 represent these three tasks respectively. Later on, the intervention team arrives at the intervention site and a new sub-phase entitled Arrival to intervention site begins at T2.1. The first step in Figure 4.12 represents this task. The CRO fulfils then the arrival to intervention site information and transmits it to the CIS and CTA operators who receive it in the CIS and CTA respectively. The communicated information at this step includes the date and time of arrival as well as the localisation of intervention team. Steps 1 and 2 in Figure 4.12 illustrate these two tasks. After having arrived at the intervention site, the intervention enters a new phase called on-site operations that starts at T3.0. Figures 4.13, 4.14, 4.15, and 4.13, represent actions, communications, and interactions during on-site operations.

As we can see in Figure 4.13, during on-site operations, rescuers access the intervention site. They start by securing places, evaluating the initial situation, and searching casualties for protecting them. The first three steps in Figure 4.13

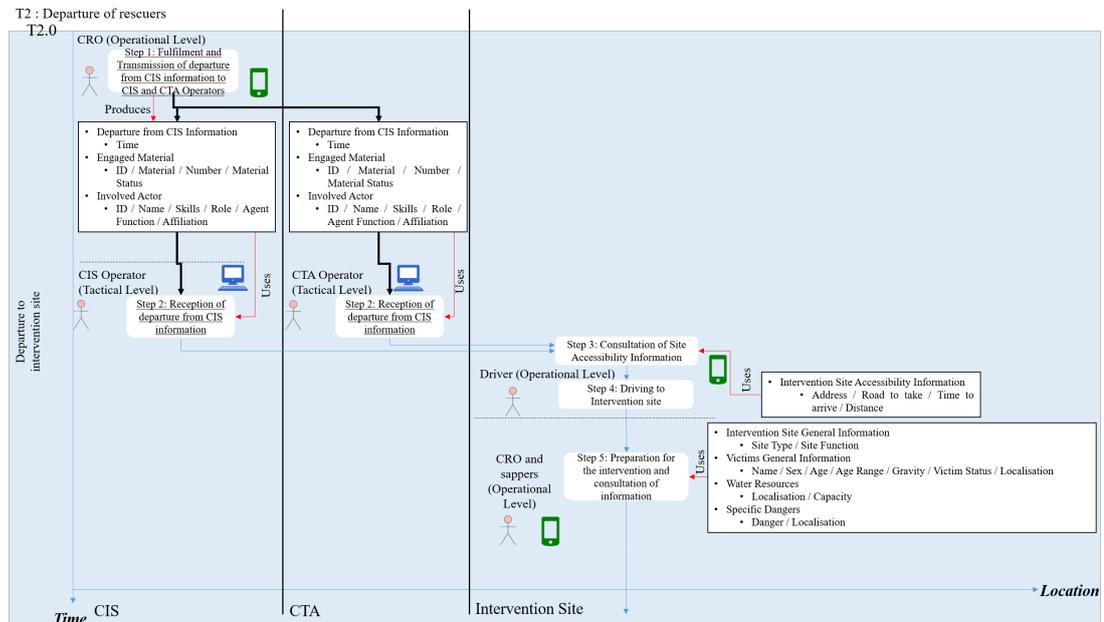


Figure 4.11: Interactions during the departure of rescuers (1).

4. MODELLING INTERACTIONS

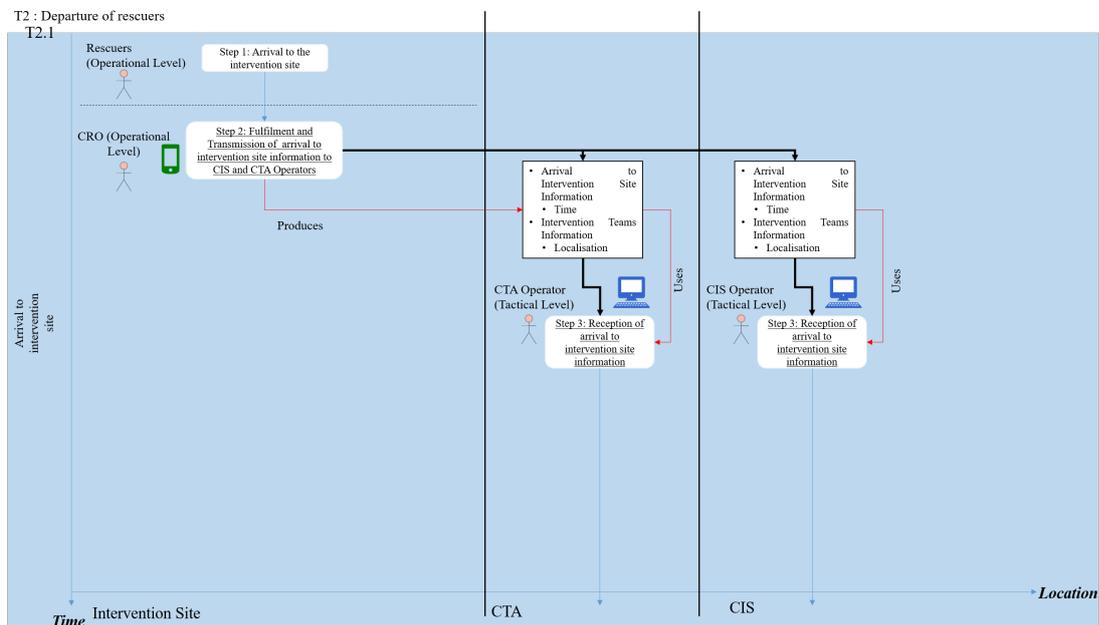


Figure 4.12: Interactions during the departure of rescuers (2).

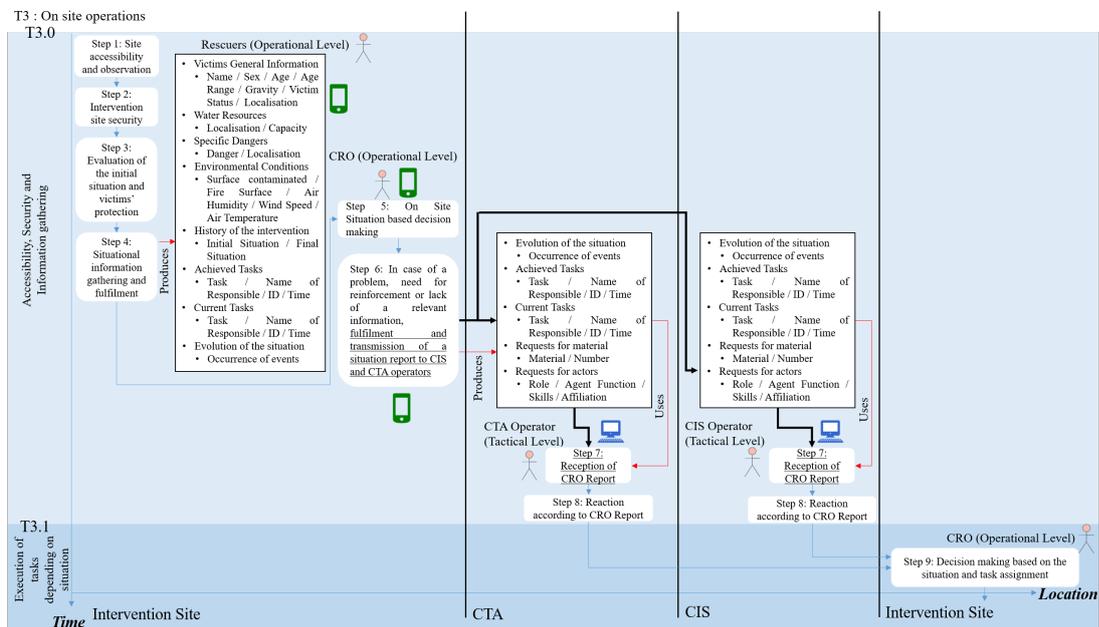


Figure 4.13: Interactions during On-site operations (1).

represent these three tasks. Then, they gather first information about the inci-

4.3 Modelling Interactions and Communications

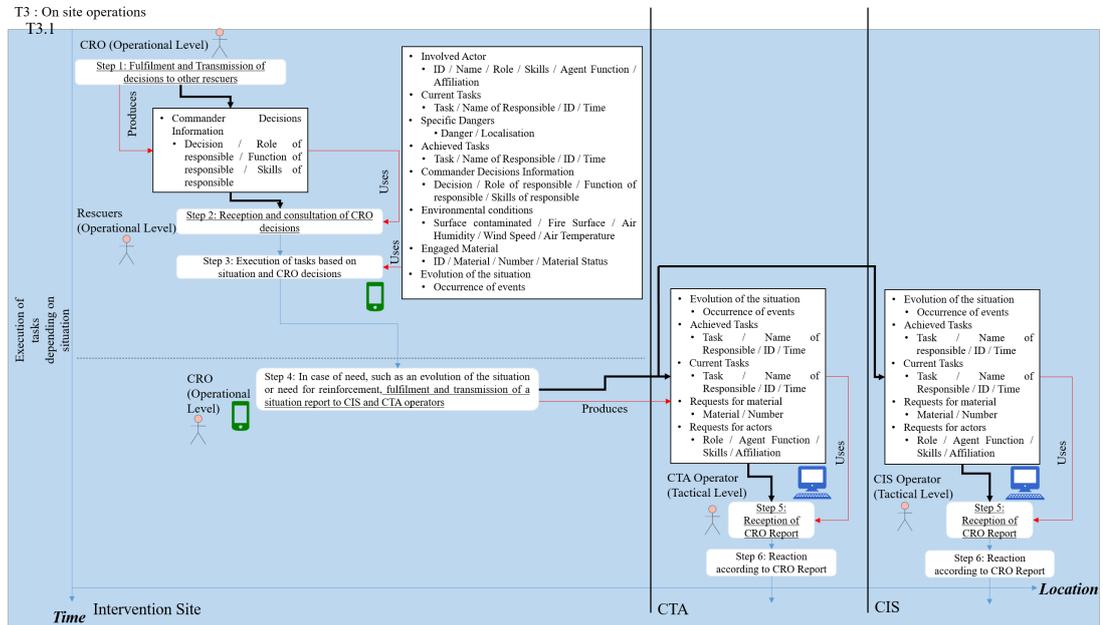


Figure 4.14: Interactions during On-site operations (2).

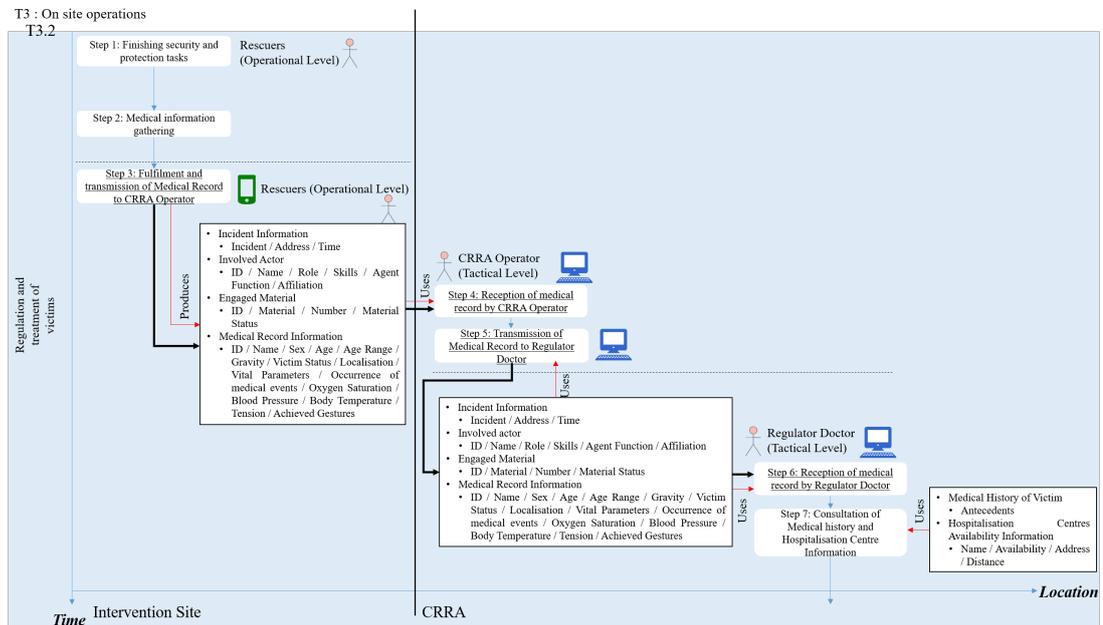


Figure 4.15: Interactions during On-site operations (3).

dent and consult the history of the intervention to evaluate the real situation and

4. MODELLING INTERACTIONS

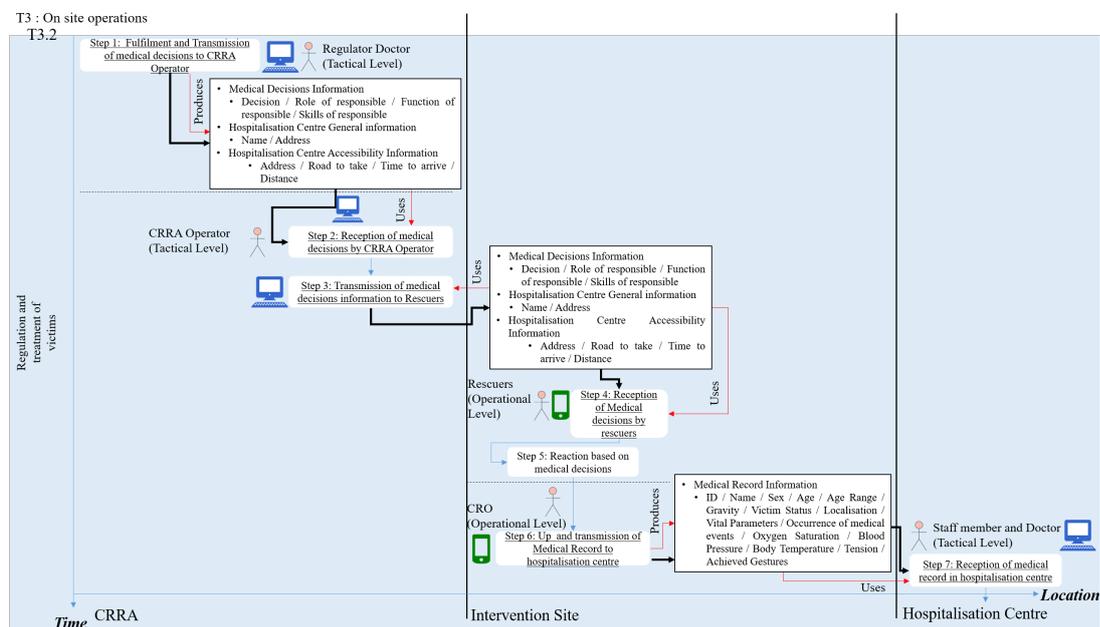


Figure 4.16: Interactions during On-site operations (4).

act appropriately. Hence, they will have access to information related to contaminated surface, involved victims, water resources and environmental conditions, achieved and current tasks, as well as the history of the intervention. This task is represented by step 4 in Figure 4.13. Based on this information, the CRO takes her/his first decisions at the operational level. In case of any problem, lack of information, or need for reinforcements, operators in CTA and CIS must be notified. Hence, the CRO fulfils a situation report through a mobile device and shares it with CIS and CTA operators who exist in CIS and CTA respectively at the tactical level. This report includes information about evolution of the situation, achieved tasks, current tasks, and requests for material and actors. Those operators will thus receive and check the CRO report through their desktops and act according to it. Otherwise, the CRO does not make any report about the initial situation. Steps 5, 6, 7, and 8 in Figure 4.13 represent these tasks respectively. At T3.1, rescuers finish the first sub-phase consisting of accessibility, security, protection and information gathering, and a new sub-phase begins at T3.2. The aforementioned sub-phase lies within the execution of tasks depending on situation. Hence, The CRO, who exists in the intervention site at the operational level, makes new decisions and assigns tasks to other rescuers based on the situation. This task is represented by step 9 in Figure 4.13. These decisions are fulfilled then

4.3 Modelling Interactions and Communications

by the CRO and transmitted to other rescuers who receive decisions information using their mobile devices. These information include commander decisions, role of responsible, function of responsible, and skills of responsible. Accordingly, rescuers start to carry out actions based on these decisions and information gathered in earlier phases. Steps 1, 2, and 3 in Figure 4.14 represent these three tasks respectively. In case of need, such as a sudden evolution of the situation or need for reinforcements, the CRO fulfils a situation report through a mobile phone and shares it with CIS and CTA operators. Those operators will thus receive and check the CRO report and act accordingly. These three tasks are represented by the last three steps in Figure 4.14. When safety, protection, and information gathering tasks are completed, the team members move to the second sub-phase of the on-site operations which consists of the regulation and treatment of victims and starts at T3.2. Therefore, those members start by collecting detailed information on the condition of the victims. Based on the collected information, the CRO fulfils a medical record through her/his mobile device. The fulfilled record includes incident information, information about involved actors and engaged materials, as well as medical record information that consists of personal and medical information about victims. The medical record is then transmitted by the CRO to the CRRA operator who exists in the CRRA at the tactical level. Hence, the CRRA receives this report through a desktop computer and transmits it to the regulator doctor who also exists in the CRRA at the tactical level. The first six steps in Figure 4.15 illustrate these tasks respectively. Moreover, the regulator doctor consults additional information related to the medical history of victims and the availability of hospitalisation centres. This task is represented by step 7 in Figure 4.15. On the basis of the consulted information, the regulator doctor takes medical decisions such as tasks to achieve, as well as decisions related to an appropriate place of reception. This task produces three groups of information that are medical decisions information, hospitalisation centre general information, and hospitalisation centre accessibility information. These information are then transmitted by the regulator doctor to the CRRA operator. Hence, the CRRA operator receives and communicates these information to the rescuers at the operational level. The first four steps in Figure 4.16 represent these tasks. According to the communicated decisions, the CRO and other members react and apply first aid gestures to the victims. Afterwards, the CRO updates the medical record and transmits it to the medical staff members and medical doctor who exist in the selected hospitalisation centre at the tactical level. Consequently, the medical staff members and doctor will receive the record and get access to the

4. MODELLING INTERACTIONS

group entitled medical record information. These three tasks are represented by steps 5,6, and 7 in Figure 4.16. Following the reception of the medical record in the hospitalisation centre, the operation enters a new phase entitled Victim's transportation starts. Figures 4.17 and 4.18 show interactions during the victims' transportation phase. As we can see in Figure 4.17, the aforementioned phase

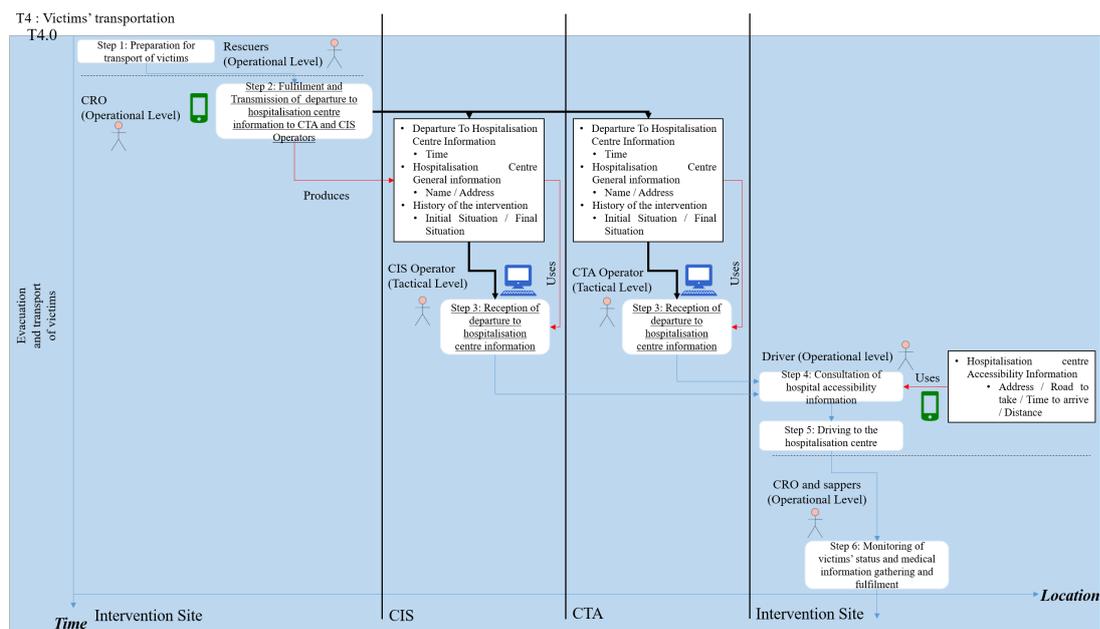


Figure 4.17: Interactions during Victim's transportation (1).

starts at T4.0 with a first sub-phase consisting of evacuation and transport of victims. During this sub-phase, rescuers start with preparing for the transport of victims. At the beginning of this sub-phase, using a mobile device, the CRO fulfils information about the departure from the intervention site and transmits it to CIS and CTA operators who exist in CIS and CTA respectively at the tactical level. The transmitted information includes the history of the intervention, hospitalisation centre general information, and departure to hospitalisation centre information such as time and date of departure. The communicated information is then received and consulted by the aforementioned operators. These tasks are represented by steps 1,2, and 3 in Figure 4.17. Afterwards, the rescuers head towards the selected hospitalisation centre. Hence, the driver drives the selected vehicle. For this aim, he consults information about hospitalisation centre accessibility such as address, road to take, time to arrive, and distance. Whereas, the CRO and other members represented by sappers monitor the victim's status.

4.3 Modelling Interactions and Communications

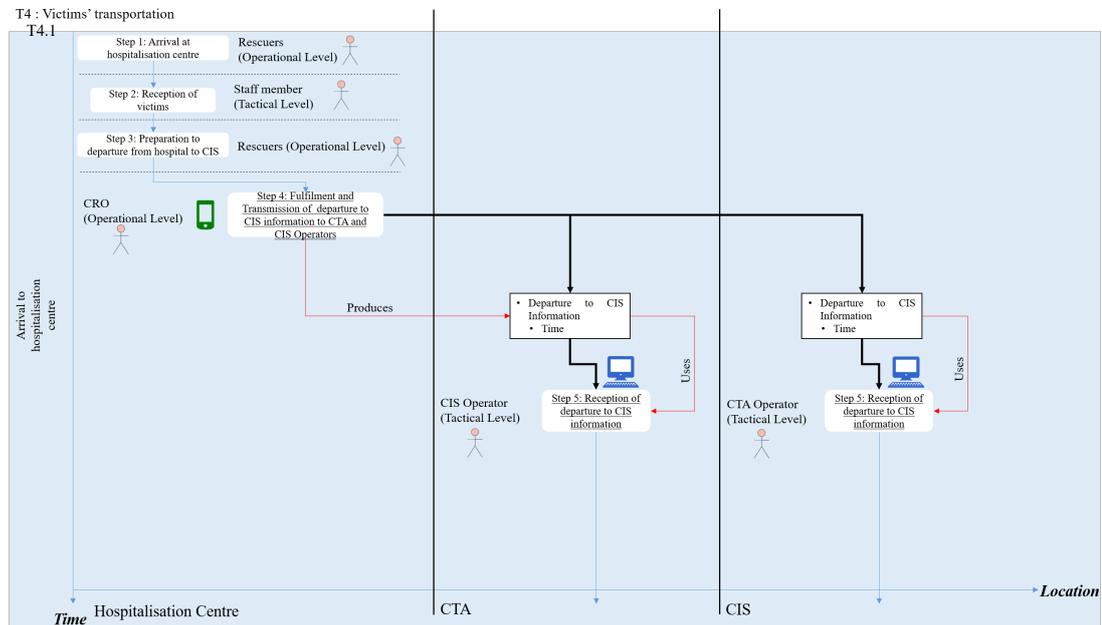


Figure 4.18: Interactions during Victim's transportation (2).

Steps 4, 5, and 6 in Figure 4.17 represent these three tasks respectively. Later on, the intervention team arrives at the hospitalisation centre and a new sub-phase entitled Arrival to hospitalisation centre begins at T4.1. During this sub-phase, rescuers arrive at the centre and medical staff members receive victims. The first two steps in Figure 4.18 represent these two tasks respectively. After the reception of victims, rescuers prepare for leaving the hospitalisation centre toward their CIS. Hence, the CRO fulfils the departure to CIS information and transmits it to the CIS and CTA operators who receive it in the CIS and CTA respectively. This communicated information at this step includes date and time of departure. These three tasks are represented by steps 3, 4, and 5 in Figure 4.18. Following these tasks, the operation enters a new phase called return and end that starts at T5.0 with departure to CIS. Figures 4.19 and 4.20, represent actions, communications, and interactions during the return and end phase. As we can see in Figure 4.19, during this sub-phase, the rescuers leave the hospitalisation centre and return to their CIS. Hence, the driver drives the selected vehicle. The first two steps in Figure 4.19 illustrate these two tasks respectively. Later on, the rescuers arrive at their CIS, and a new sub-phase entitled Arrival in CIS begins at T5.1. During this sub-phase, information about the arrival is transmitted to the CIS and CTA operators by the CRO. Hence, the aforementioned operators

4. MODELLING INTERACTIONS

receive the communicated information in their centres at the tactical level. These three tasks are represented by steps 4, 5, and 6 in Figure 4.19. Eventually, the CRO fulfils and archives an intervention report, and the intervention arrives at its end. This archived report includes the majority of information exchanged during the intervention such as departure and arrival information, incident information, engaged material and actors, medical record information, achieved tasks, and hospitalisation centre general information. Steps 1 and 2 in Figure 4.20 represent these tasks.

From the model presented in figures 4.8 to 4.20, we can see how involved actors interact with each other depending on the actions and the situation. Moreover, we can see the needed or produced information in each step together with the device used to exchange it. In addition, we can easily extract dependencies between Actor, Action, Information, Communication device, Operation phase, Location, and Time. Moreover, we can simply see the information flow between the operational level and tactical level in rescue operations. Furthermore, this model serves as a basis to define the communication system specifications based on communication protocols defined in rescue operations and thus, to support the representation of situations. The proposed model is built on the basis of the communication and process protocols described in the domain-related documentation. Its application

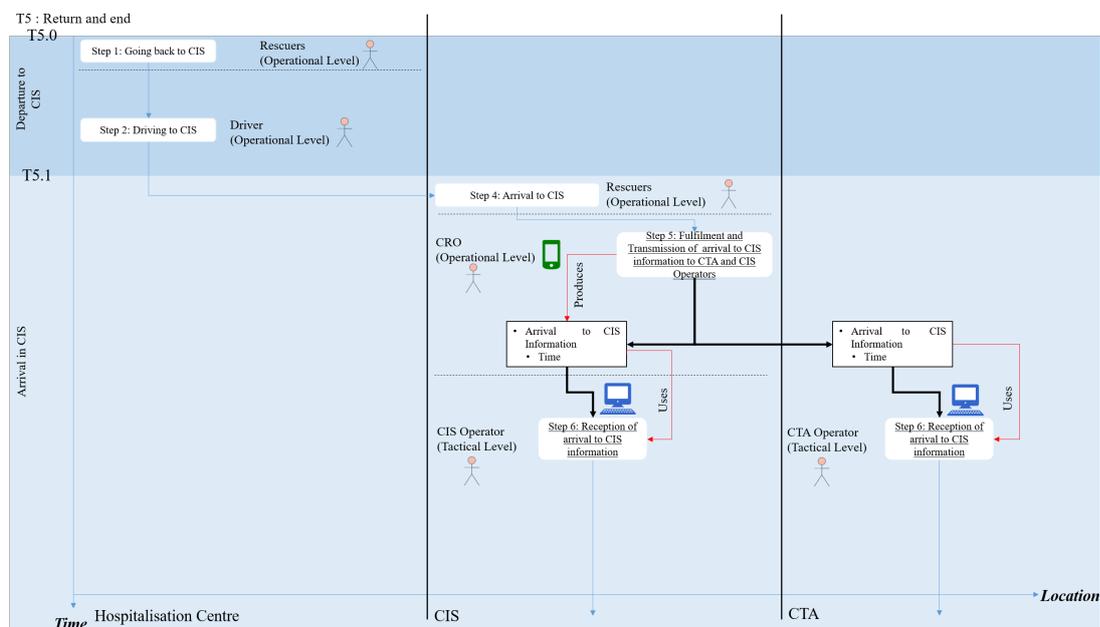


Figure 4.19: Interactions during the return and end phase (1).

4.3 Modelling Interactions and Communications

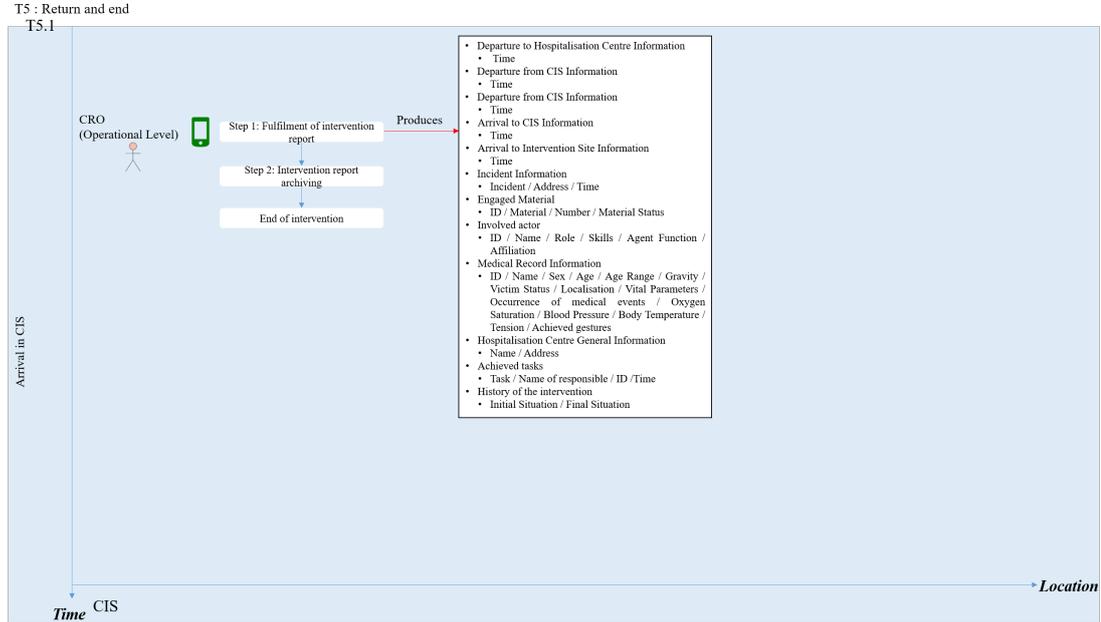


Figure 4.20: Interactions during the return and end phase (2).

is limited to daily rescue operations. The work presented does not cover large-scale and disaster response. In the French case, several documents that describe the rescue response procedure were elaborated by the state. However, there is no specific plans that are applied in this case. Some plans were elaborated and can be activated such as ORSEC, the NOVI plan, and the white plan [Elmhadhbi, 2020]. However, the application of those plans is specific to particular cases and is not related to daily rescue operations. The plan ORSEC provides the general framework of the response process in large-scale events such as disasters. The NOVI is the reference plan for the on-site mass causality management. Regarding the white plan, it is used to identify a set of hospitals where the victims can be transported in case of large-scale events that cause a large number of victims. The activation of those plans require the involvement of additional actors such as mayors and prefects who are not involved in daily rescue operations. In addition, changes in activities described in the model presented can occur in real practices. Indeed, different actors that participate in rescue operations have different levels of knowledge and experience related to the practices in the field. Consequently, the actors can react in different ways during the interventions according to their levels of expertise. Unfortunately, like any existing model, the proposed model cannot cover all of the changes that may occur during the interventions in terms

4. MODELLING INTERACTIONS

of activities since most of these changes depends on the level of the expertise of the user, as well as the sudden events that may occur. This can be solved through the flexibility and the personalisation of the communication system that can be adapted to the preferences and the level of experience of its user. For instance, two users with the same role can have different interfaces on the basis of their preferences and experience. Moreover, in the proposed system, we are not imposing the application of different activities described in the model in a sequence order. The activities are modelled but their sequence can be changed during the interventions. A detailed description of the proposed communication system is provided in Chapter 6.

4.4 Conclusions

As it has been mentioned in Chapter 3, we propose in this thesis an approach for designing a communication system that aims at supporting situation awareness in daily rescue operations. The proposed approach follows a five-step methodology. The first step in the proposed approach consists in analysing and modelling communications and interactions in these operations through the study of documents, reports, and legislation related to the domain. This study allows us to identify different services as well as their missions, to analyse procedures, and to link these missions with interactions. Moreover, this study leads to identifying the requirements, criteria, and practical needs of actors on the basis of their practices. Furthermore, it helps to represent those procedures and interactions in a formalised way. Unfortunately, for reasons related to time and confidentiality, we were unable to access the field in order to analyse the real practices of the rescue actors. Therefore, we are totally aware of the limits of our analysis. In this chapter, we focused on the first step of the proposed approach. In this context, we introduced first organisations and services involved in French daily rescue operations as well as their missions. Moreover, we presented an organisational chart that shows the different organisational levels as well as a general flow of information and decisions between different levels. We then described a scenario of a rescue operation derived from practices applied in France. This scenario serves as a basis for our study. Afterwards, we identified required elements and parameters to be taken into account when modelling interactions in complex contexts such as rescue operations. Those elements are *Actors*, their *Roles* and their *Positions*

in the organisational levels of operations, *Information*, *Communication instrument*, *Tasks*, *Time*, and *Location*. In addition, we presented the main phases of a rescue operation. Moreover, we proposed a structural model based on those requirements. Eventually, we proposed an interaction model that shows interactions between different actors in French rescue operations. This model allows efficient extraction of dependencies between Actor and Role, Task, Information, Communication device, Operation phase, Location, and Time. In addition, it allows simple visualisation of the information flow between the operational level and tactical level in rescue operations. Moreover, this model serves as a basis to define the communication system specifications based on communication protocols defined in rescue operations and thus, to support the representation of situations. However, it does not cover all of the uncertainties that may occur in terms of activities and information since most of these uncertainties cannot be predicted in the aforementioned protocols. Regarding the rescue model as well as the proposed requirements, an approach based on activities and procedures derived from rescue operations applied in France has been presented. However, the obtained results can be adopted for use and application in other countries since the main elements, parameters, and requirements are generic.

After having modelled interactions, let us move to the next step of the approach presented in Chapter 1. The aforementioned step lies within the construction of an application ontology that represents the knowledge required for designing a communication system oriented for rescue actors that guarantees the confidentiality of information. In order to propose a usable system that is based on operational practices, we develop this ontology based on the interaction model presented in this chapter. Hence, we present in the next chapter the proposed ontology as well as the adopted methodology for its development.

4. MODELLING INTERACTIONS

Chapter 5

ResOnt Ontology

Contents

5.1	Introduction	122
5.2	Proposed solutions	123
5.3	Methodology of Ontology Development	125
5.3.1	Specification	128
5.3.2	Conceptualisation	132
5.3.3	Formalisation and implementation	139
5.3.4	Evaluation	141
5.3.5	Maintenance	142
5.4	ResOnt Ontology Description	143
5.4.1	ResOnt Rescue and Communication Module	143
5.4.2	ResOnt Design Module	146
5.4.3	ResOnt Access Control Module	149
5.4.4	Complete ResOnt Ontology	151
5.5	Conclusions	155

5.1 Introduction

As it has been mentioned in Chapter 3, we propose in this thesis an approach for designing a communication system that aims at supporting situation awareness in rescue operations. The proposed approach follows a five-step methodology illustrated in Figure 1.1. In Chapter 4, we presented the first step of the proposed approach that consists in modelling interactions and communications in these operations. As we can see in Figure 1.1, the second step in the proposed approach lies within the construction of an application ontology that represents the knowledge required for designing a communication system oriented for rescue actors that guarantees confidentiality of information. When designing a communication system oriented for rescue actors, there are several aspects and dimensions to take into consideration. First, since the system is oriented to support information exchange and awareness, it is essential to consider different practices and interactions as well as elements required for supporting awareness. Second, it is strongly required to consider the design and the usage of the system in real practices. Third, since a great amount of exchanged information in rescue operations is personal information, it is required to consider confidential access to information. Hence, at a second step, we propose an application ontology that covers those aspects. This ontology is referred to as ResOnt that stands for Rescue Ontology. It is mainly based on the interaction model proposed in Chapter 4. Indeed, the use of ontological approaches can facilitate the explainability and the dynamic exploitability of the interaction model. The proposed ontology consists of three modules. The first module is oriented for representing knowledge related to communications and practices in rescue operations. It serves for ensuring a common perception and understanding of situations between collaborating stakeholders as well as representing and formalising different procedures and flow of information. The second module incorporates the knowledge required for the dynamic design and configuration of the system and interfaces. Whereas, the third module is specific for representing knowledge required for guaranteeing access control and rights management in the system. In this chapter, we present the methodology adopted for developing the ontology. In this context, different steps in this methodology are discussed. We then describe ResOnt ontology in detail. Hence, we present its three modules, the concepts of each module, as well as different relations between concepts. Moreover, we present different ontologies that we reused to develop ResOnt. Eventually, we present the complete ontology obtained after the integration of those three modules. We notice that we do not

aim, in this work, to develop complete domain ontologies for each one of the three domains of interest. This work is limited to the creation of a knowledge base that includes the required knowledge for designing a communication system oriented for rescue actors.

5.2 Proposed solutions

The problem treated in our work is mutual awareness in a complex and dynamic domain that is the domain of rescue. We especially address effective information sharing and communication as a first brick towards helping this awareness. The research project presented in this thesis is part of the definition of a flexible system that improves information sharing, the first support for awareness in collaborative work in an emerging, complex and dynamic domain, which is the domain of rescue. This system shall be designed in a way that guarantees mutual awareness between different stakeholders. Moreover, the system must ensure effective communications and confidential access to information. Finally, it is of great importance to design the system in a way that gains stakeholders acceptability and that makes it appropriate to their practices. In Chapter 1, three research questions were formulated:

Q.1: How to guarantee mutual awareness of situations between different participating actors in rescue operations?

Q.2: How to guarantee effective communications and confidential access to information in rescue operations?

Q.3: How to guarantee the acceptability of the proposed system by its end-users?

Moreover, three corresponding solutions were presented in Chapter 1. The first solution consists in enhancing interactions and information exchange through a communication support system based on semantic representation techniques and ontologies. This latter aims at ensuring a common perception of situations amongst involved stakeholders. The second solution relies on taking the real practices and interactions into consideration in the design of the system. This solution also consists in choosing relevant confidentiality policies and mechanisms in a way that meets the stakeholders' needs. This will help to develop an operational system that can be used by operational units for the support of their tasks. Whereas,

5. RESONT ONTOLOGY

the third solution consists in guaranteeing the acceptability of the system by its end-users by proposing an approach through which those users can design the system in a customised way based on a semantic representation of knowledge. This approach will also help to enhance the flexibility and adaptability of the proposed system. Based on those solutions and the review of literature, we identified several criteria that an effective and usable awareness and communication-support system has to meet. These criteria include: **Taking into consideration the diversity of stakeholders' needs, personalisation and adaptability to users' contexts, flexibility and adaptability**, and eventually, **guaranteeing confidentiality information**. We would like to remember that the stakeholders' needs include: **Common terminology, Interoperable communications between all the services, Exchange of different required types and forms of information, Resources allocation, Exchange of actionable information based on contexts**.

Hence, we propose to adopt an ontology-based approach to design a communication and awareness-support system that meets the aforementioned solutions and criteria. To this end, we propose an application ontology called ResOnt that constitutes an essential element in the proposed approach. ResOnt helps to develop a system that meets the identified criteria and responds to the stakeholders' needs by:

- Ensuring a common interpretation of information between different stakeholders with a common terminology. This will help to ensure a common perception and understanding of situations between stakeholders which will enhance situation awareness.
- Representing and formalising different procedures and flow of information. Thanks to this representation, ResOnt will help to develop a system that is based on practices, interactions, and needs. Moreover, it will help to dynamically exploit the interaction model.
- Representing knowledge required for managing access rights and guaranteeing confidentiality of information in the system to develop. This will help to guarantee the confidentiality of information.
- Representing knowledge required for the dynamic design and configuration of the system and interfaces. This will facilitate the flexibility and adaptability of the system to different usages. Moreover, it constitutes an essential step toward the personalisation of system interfaces.

5.3 Methodology of Ontology Development

Hence, ResOnt ontology considers several aspects and dimensions mainly communications and interactions, design, and access control. To this end, we propose to construct ResOnt ontology based on three different modules. Moreover, we import those three modules and we define relations between their concepts in order to obtain the complete application ontology ResOnt. We notice that the aforementioned modules are interdependent. The aim of this modularisation is limited to the separation and classification of different concepts and relations based on distinct areas and aspects. The ontology modules are:

- ResOnt Rescue and Communication module. This module incorporates required concepts and relations to formalise practices and interactions in rescue operations. It also serves for ensuring a shared understanding of situations amongst different stakeholders.
- ResOnt Design module. This module includes concepts and relations needed to design a communication system in a flexible and personalised way.
- ResOnt Access Control module. This latter includes concepts and relations required for controlling access and rights management.

5.3 Methodology of Ontology Development

In this section, we present the methodology adopted to create the proposed application ontology. Creating an ontology is not an easy task nor a straightforward one, especially when ontologies become more relevant and more complex [Corcho *et al.*, 2004; Masmoudi *et al.*, 2020]. Therefore, a methodology that guides the creation of ontology and manages it is essential. However, one of the most challenging problems is how to select the right approach, taking into account the complexities of the domain to be modelled, and the furthest reuse of the ontology. To support ontologies building, several methodologies such as METHONTOLOGY, On-to-knowledge, and Activity First Methodology, have been discussed in Chapter 3. Moreover, several studies were conducted to compare and evaluate ontology development methodologies [Al-Baltah *et al.*, 2014; Corcho *et al.*, 2003; De Nicola *et al.*, 2009; Iqbal *et al.*, 2013; Mizoguchi, 2004; Pinto & Martins, 2004]. According to [Pinto & Martins, 2004], an effective methodology must include a set of stages through which an ontology is build. This set represents the common ontology life cycle and includes similar steps to those defined in the IEEE 1074-1995 standard processes [Schultz *et al.*, 1997]. The ontology stages consists of

5. RESONT ONTOLOGY

several activities: Specification, Conceptualisation, Formalisation, Implementation, and Maintenance, Knowledge acquisition, Evaluation, and Documentation. Table 5.1 shows a comparison of ontologies development methodologies against the common ontology life cycle. As we can see in Table 5.1, among the selected

Table 5.1: Comparison of ontologies development methodologies against the ontology development life cycle.

Activities	METHONTOLOGY	On-to-Knowledge	AFM	TOVE	UPON
Specification	✓	✓	✓	✓	✓
Conceptualisation	✓	✓	✓	p	✓
Formalisation	✓	✓	✓	✓	✓
Implementation	✓	✓	✓	✓	✓
Maintenance	p	p	x	x	p
Knowledge Acquisition	✓	x	✓	p	✓
Evaluation	✓	✓	x	x	✓
Documentation	✓	✓	✓	x	✓

✓:supported; x:unsupported; p:partially supported

methodologies, METHONTOLOGY and UPON are the most ones that respect the ontology life cycle. The two aforementioned methodologies include different activities defined in the life cycle. However, UPON requires the involvement of domain experts and knowledge engineers in the development phase. Therefore, in this work, we adopt the METHONTOLOGY to develop the proposed

5.3 Methodology of Ontology Development

ontology [Fernández-López *et al.*, 1997] since in this work we did not have the opportunity to meet domain experts. This choice is also argued by the fact that METHONTOLOGY is the most mature one amongst the existing methodologies [Corcho *et al.*, 2003]. Indeed, METHONTOLOGY has been recommended by the Foundation for Intelligent Physical Agents (FIPA) for the ontology construction task [Corcho *et al.*, 2003]. Moreover, it has been applied into a large number of projects. Figure 5.1 shows the main activities and steps of ontology development as defined in METHONTOLOGY. As shown in Figure 5.1, METHONTOLOGY defines several activities required for building an ontology. Those activities are classified into three categories: *Management Activities*, *Development Activities*, and *Support Activities*. Management Activities consist of the planification that is the first activity toward the ontology development. Regarding the development activities, they include five distinct activities that are: Specification, Conceptualisation, Formalisation and Implementation, and Maintenance. Whereas, support activities incorporate Knowledge acquisition, Evaluation, and Documentation. Those latter are carried in parallel with different development activities.

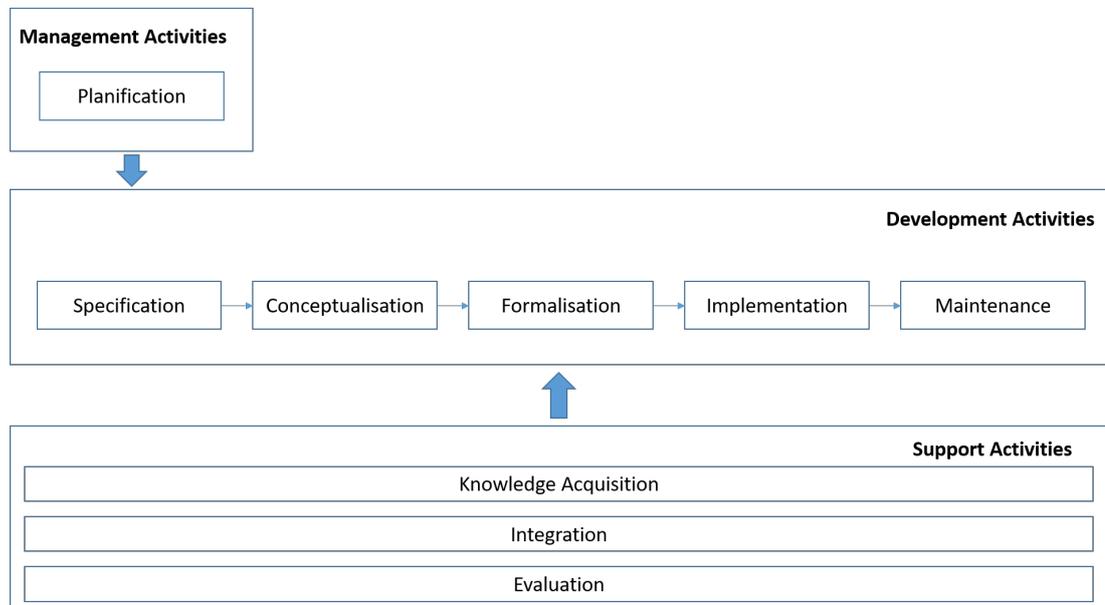


Figure 5.1: Methontology steps for ontology construction.

*Figure adapted from [Fernández-López *et al.*, 1997].

5. RESONT ONTOLOGY

5.3.1 Specification

The purpose of the specification activity is to create either an informal, semi-formal or formal document of ontology specification written in natural language, using competency questions or using a collection of intermediate representations, respectively [Fernández-López *et al.*, 1997]. In this context, we start by identifying the purpose of this ontology.

5.3.1.1 Ontology purpose

Based on the proposed solutions, ResOnt is an application ontology that aims at representing the knowledge required for designing a communication and awareness-support system oriented for rescue actors that guarantees the confidentiality of information (Cf. Section 5.2). It serves for ensuring a shared perception and understanding of situations between collaborating actors. In addition, it helps to design a communication system in a flexible and personalised way that is adapted for usage. Moreover, it serves for controlling access control and rights management in the system. After having fixed the ontology objectives, we move to the ontology specification. To this end, we adopt Competency questions (CQs) as a technique to define the ontology specifications.

5.3.1.2 Competency Questions

Competency questions play an important role in the ontology development life-cycle as they represent the ontology requirements [Bezerra *et al.*, 2013]. They consist of a set of questions stated in natural language that the ontology must be able to answer [Noy & Hafner, 1997]. For clarity and simplicity, we classify the competency questions defined in ResOnt into three categories: (1) CQs related practices and interactions in rescue operations; (2) CQs related to the design of system and interfaces; (3) CQs related to access control. We first start with questions related to practices and interactions in rescue operations. In this context, we defined a total of thirty-two Competency questions presented in Table 5.2. Those questions were mainly defined on the basis of the interaction model described in Chapter 4.

5.3 Methodology of Ontology Development

Table 5.2: Competency questions related to practices and interactions in rescue operations.

CQi	Competency Question
1	What are the possible types of an incident?
2	What are the different Functions that organisation members could have?
3	What are the Organisations involved in French rescue operations?
4	What are the different Organisation Member Roles that organisation members could have?
5	What are the different Groups of Information that are fulfilled, exchanged, or archived during an intervention?
6	What is (are) the Group(s) of Information that a Task [X] uses?
7	What are the different Tasks that an Organisation Member could execute?
8	What is (are) the Group(s) of Information that a Task [X] produces?
9	What is (are) the Information that a Group of Information [X] has?
10	What are the possible Communication Instruments that an Organisation Member could use?
11	What are the different Phases of an intervention that Have a participating Organisation member role [X]?
12	What are the Different Sub-Phases that a phase [X] has?
13	What are the Different Sub-Phases of an intervention that Have a participating Organisation member role [X]?
14	What is (are) the Task(s) that occurs during a Sub-Phase [X]?
15	What is the Time Instance that a Sub-Phase [X] Starts On?
16	What are the Possible Locations of Tasks during an Intervention?
17	What Location is the place of a Task [X]?
18	What Task(s) is (are) associated with an Organisation Member Role [X]?

5. RESONT ONTOLOGY

19	What are the different Material that an Organisation member could use in an intervention?
20	What are different Status that a Material could have?
21	What are different Site Functions that an Intervention site could have?
22	What is the Availability of an Object?
23	What are the different Skills that Organisation members could have?
24	What are the different Affiliations that Organisation members could have?
25	What are the different Grades that Organisation members could have?
26	What is the Age Range that a Victim could have?
27	What are different Types that an Intervention site could have?
28	What is the Sex that a Victim could have?
29	What are the possible Roles of a responsible for a certain Task?
30	What are the possible Functions of responsible for a certain Task?
31	What are the possible Skills of responsible for a certain Task?
32	What is the Victim Status that a Victim could have?

Moreover, we defined several questions related to the design of the system and interfaces. In this context, a total of eleven questions were defined as shown in Table 5.3. Eventually, we defined several Competency questions related to access control and rights management. A total of four questions were defined in this context as shown in Table 5.4. After having defined the ontology objectives and specified the ontology through a set of competency questions, we move to the knowledge acquisition phase.

5.3.1.3 Knowledge acquisition

This phase consists in acquiring knowledge using in conjunction techniques such as formal and informal analysis of texts, interviews, brainstorming, and knowledge acquisition tools. Unfortunately, in this work, we did not have the opportunity

5.3 Methodology of Ontology Development

Table 5.3: Competency questions related to the design of the system and interfaces.

CQi	Competency Question
1	What are the Main elements to consider for designing an interface based on context?
2	What is the Computational functionality that a Task [X] is attached to?
3	What is the Data Type that an Information could have?
4	What is the Interface Component that an Information can have?
5	What is the Field Type that an Information can have?
6	What is the Orientation that an Information can have?
7	What is the Degree of criticality that an Information can have?
8	What is the Category that an Information can have?
9	What is the Interface that a Communication Instrument [X] Could have?
10	What is the Interaction Way defined by a Functionality [X]?
11	What are the Dimensions of an Interface [X]?

Table 5.4: Competency questions related to access control and rights management.

CQi	Competency Question
1	What is the Relation between an Organisation Member Role [X] and a Group of Information [X] in terms of Access Rights?
2	What is the Relation between an Organisation Member Role [X] and a Group of Information in terms of Privacy?
3	What are the different Access Types?
4	What are the Possible Actions that can be executed on Information?

to meet domain experts who were supposed to help in the knowledge acquisition and the ontology evaluation steps. Hence, we propose to develop the required ontology based on domain-related documentation as well as existing ontologies.

5. RESONT ONTOLOGY

To do so, a deep analysis of the domain of rescue was made based on documents, reports, legislation, and ontologies related to the domain. Moreover, we analysed interactions and practices based on the interaction model presented in Chapter 4. On the other hand, we conducted a study of approaches and existing ontologies related to the design of systems. Similarly, several existing studies and ontologies related to access control were analysed to capture the required knowledge in this context. Those studies allowed us to acquire a specific and detailed knowledge about the required concepts, their properties, and their relationships. Following the specification phase, we move to the next step in the ontology development methodology. The aforementioned step, so-called Conceptualisation is presented in the next subsection.

5.3.2 Conceptualisation

Conceptualisation consists in structuring the domain knowledge in a conceptual model or a conceptual ontology. This latter aims at describing knowledge related to a certain domain in terms of the domain vocabulary identified in the ontology specification activity [Fernández-López *et al.*, 1997]. As a first step, we identified three modules to encapsulate the knowledge related to each part of designing a customised communication-support system oriented for rescue actors that guarantees the confidentiality of information. Those modules are ResOnt Rescue and communication module, ResOnt Design module, and ResOnt Access control module. We would like to remember that the aforementioned modules are interdependent. The aim of this modularisation is limited to the separation and classification of different concepts and relations based on distinct areas and aspects.

5.3.2.1 ResOnt modules

An important step in the conceptualisation phase consists in identifying terms and units in a domain, extracting their meanings, giving complete definitions to these terms, and then expressing differences and similarities of each term or unit with respect to its parents and siblings. The result of this step is a first taxonomy of concepts, which can be modified during the definition of properties and relations with other concepts. Following the definition of concepts, it is essential to define properties and relations between concepts classified into the taxonomy obtained in the first step. Accordingly, we defined the required concepts in each

5.3 Methodology of Ontology Development

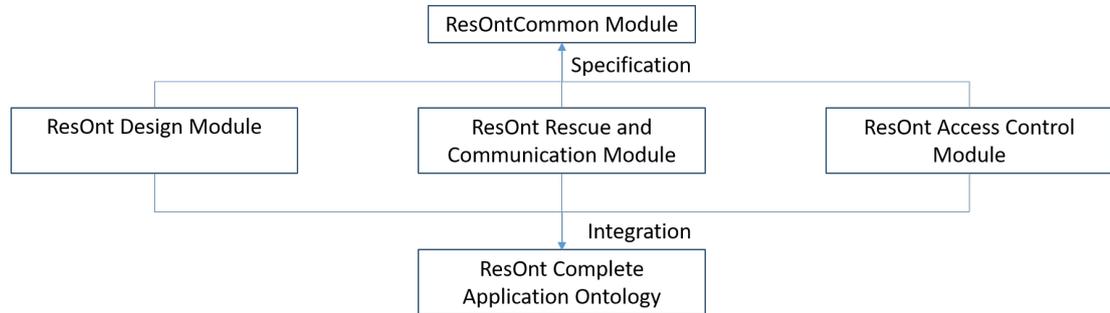


Figure 5.2: Different modules of ResOnt Ontology.

module on the basis of the knowledge acquired from documents, existing ontologies, and domains-related documentation. Moreover, in order to create a complete application ontology, it is necessary to define relations between concepts and to integrate the three defined modules. To this end, we propose to create a common module called ResOnt Common as it has been done in [Elmhadhbi *et al.*, 2019] and suggested in [Özacar *et al.*, 2011]. The proposed common module incorporates the general concepts that different modules use. ResOnt Common module can be then specified to construct the three modules separately. According to [Elmhadhbi *et al.*, 2019], defining a common module makes the integration of distinct ontological modules easier. Figure 5.2 illustrates the modules of ResOnt ontology. As we can see in Figure 5.2, we start with the construction of the ResOnt Common Module. This latter is then specified and extended to create three ontological modules respectively: ResOnt Rescue and Communication module, ResOnt Design module, and ResOnt Access Control module. The resulting three modules can be then integrated in order to obtain a complete application ontology. In order to develop a relevant, reusable, and consistent ontology, several general principles were considered. Those principles were mainly defined in [Arp *et al.*, 2015]. According to [Arp *et al.*, 2015], a good ontology will be one that is developed in such a way to respect those principles. One of the most general principles to respect during an ontology development is the principle of reusing existing ontologies. Hence, during the development phase, existing top-level as well as classes from mid-level and domain ontologies must be reused if possible [Elmhadhbi, 2020]. Indeed, with the intent of accelerating and enhancing the development of an ontology, it is recommended to reuse existing ontologies instead of beginning from scratch [Fernández-López *et al.*, 1997]. In this context, several existing studies adopted the reuse of top-level, mid-level, and domain ontologies

5. RESONT ONTOLOGY

as a first step toward the development of new domain and application ontologies [Ali *et al.*, 2019; Elmhadhbi *et al.*, 2019; Masmoudi *et al.*, 2020; Portelli *et al.*, 2019; Semy *et al.*, 2004]. Top-level or fundamental ontologies can be understood to provide ontology developers with a sound basis on which they can focus and re-use. An important explanation for the employment of top-level ontologies is their standardising nature, which will ensure the true interoperability of ontologies [Schulz & Boeker, 2013]. Moreover, their use simplifies the alignment between domain ontologies. It allows more effective governance of ontology development [Arp *et al.*, 2015]. Regarding mid-level ontologies, they serve as a bridge between abstract concepts defined in top-level ontologies and more specific concepts defined in domain and application ontologies. Also-called core references ontologies, mid-level ontologies have a common goal that consists in providing a mechanism to facilitate the mapping and reuse of concepts across distinct domains. Those ontologies may include more explicit representations of abstract concepts contained in the top-level ontologies. Moreover, they often include a collection of ontologies that describe widely used concepts, such as Time and Location [Semy *et al.*, 2004]. Accordingly, we propose to reuse a top-level ontology and a mid-level ontology and classes from several existing domain ontologies as an essential step to create a reusable ontology that can be interoperable with or reusable by other ontologies. In 5.3.2.2, we provide more details about the top and mid-level ontologies reused in our case.

5.3.2.2 Reused ontologies

In order to reuse top-level and mid-level ontologies, it is required to select relevant ontologies that are appropriate to the domain of application. Several top-level ontologies have been proposed in the literature. The most well-known top-level ontologies are DOLCE [Gangemi *et al.*, 2002], SUMO [Pease *et al.*, 2002], and BFO [Arp *et al.*, 2015]. Of the three leading aforementioned ontologies, BFO is in one respect the most appropriate for the requirements of scientific users [Smith & Ceusters, 2010]. This is because BFO is a strict ontology that does not contain its representation of chemical, psychological, biological, or other types of entities [Smith & Ceusters, 2010]. Moreover, since the domain of rescue is a realistic domain, it is necessary to select a realist top-level ontology. This means that the ontology should be able to represent the world entities as they are in reality [Masmoudi *et al.*, 2020]. Furthermore, in order to ensure that the ontology can be extended to an application ontology oriented for rescue operations, it should

5.3 Methodology of Ontology Development

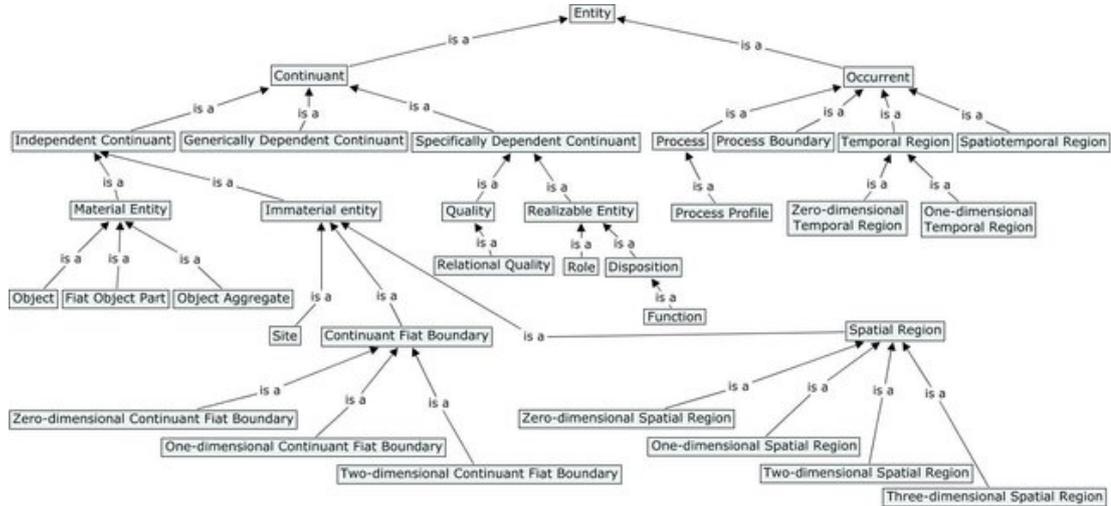


Figure 5.3: BFO 2.0 is-a hierarchy.

*Figure source: [Smith *et al.*, 2015]

include universal classes [Elmhadhbi *et al.*, 2018]. Universal classes are general entities that generalise or abstract over similar particular things. Person, process, and location are examples of universal classes [Semy *et al.*, 2004]. From the above-mentioned ontologies, SUMO and DOLCE classify particulars while BFO classifies universals [Semy *et al.*, 2004]. Consequently, we propose the reuse of BFO as a top-level ontology since it is universal and realist [Dumontier & Hoehndorf, 2010]. Moreover, BFO's well-documented guidance, its extensive use in hundreds of biomedical and military projects, and increasingly being adopted in emergency response domains are further factors that justify the selection of BFO. Figure 5.3 shows the is-a hierarchy of BFO in its version:2.0. implemented using the OWL-2 Language. As we can see in Figure 5.3, an entity, in BFO classification, is divided into *Occurrent* and *Continuant*. An occurrent entity is an entity that has temporal parts and that happens, unfolds, or develops through time [Kougias *et al.*, 2015]. Examples of occurrent entities are process, temporal region, process boundary, and spatiotemporal region. Whereas a continuant entity is an entity that exists in full at any time in which it exists at all, persists through time while maintaining its identity, and has no temporal parts [Kougias *et al.*, 2015]. Resource, agents, and material are examples of continuant entities. Besides their classification, each one of the BFO classes presented in Figure 5.3 was also defined in BFO as shown in Table 5.5. Table 5.5 summarises the definitions of the eight meta-classes of BFO. Regarding mid-level ontologies, several

5. RESONT ONTOLOGY

Table 5.5: Definitions of BFO’s meta-classes.

BFO’ Class	Definition
Entity	Anything that exists or has existed or will exist.
Occurrent	An entity that has temporal parts and that happens, unfolds or develops through time.
Continuant	An entity that exists in full at any time in which it exists at all, persists through time while maintaining its identity and has no temporal parts.
Process	An occurrent that has temporal proper parts and depends on some material entity at instance t.
Process boundary	A temporal part of a process.
Temporal region	An occurrent entity that is part of time as defined relative to some reference frame.
Spatiotemporal region	an occurrent entity that is part of space-time.
Independent Continuant	A continuant that is a bearer of quality and realisable entity entities, in which other entities inhere and which itself cannot inhere in anything.

ontologies have been proposed in the literature such as OWL Time Ontology [Hobbs & Pan, 2006], Geonames [Frontini *et al.*, 2013], the Mid-Level Ontology (MILO) of SUMO [Pease *et al.*, 2010], Hydontology ontology [Blázquez *et al.*, 2007], the Customer relationship domain ontology [Magro & Goy, 2012], and Common Core Ontologies (CCO) [Rudnicki, 2017]. Amongst these ontologies, we choose to reuse the CCO as it has been done in [Elmhadhbi *et al.*, 2019; Masmoudi *et al.*, 2020; Mohd Ali *et al.*, 2020; Morosoff *et al.*, 2015]. The goal of CCO is to provide a suite of ontologies that can be extended to represent the knowledge of multiple domains. The reason behind choosing CCO is two-folded. On one hand, CCO extends the BFO top-level ontology framework. The BFO framework incorporates the BFO ontology that is the selected top-level ontology in our case. Moreover, this framework includes the Relation Ontology (RO) that defines relations between concepts at a high level. On the second hand, thanks to its multiple ontologies, CCO can be simply extended to create an application on-

5.3 Methodology of Ontology Development

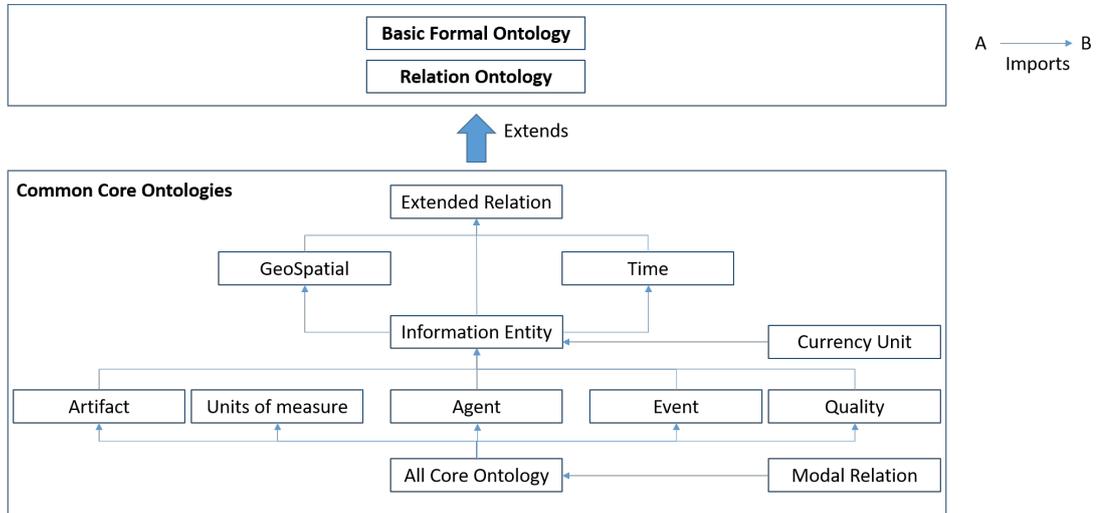


Figure 5.4: CCO Ontologies and importation structure.

*Figure adapted from [Rudnicki, 2017]

tology that covers distinct aspects and domains. Moreover, CCO is a set of realist ontologies, which is required for building an ontology related to the domain of rescue. Similarly to BFO, CCO is implemented using the OWL-2 language. Figure 5.4 shows the different ontologies and the importation structure in CCO. As we can see in CCO Figure 5.4, CCO reuses BFO and RO ontologies. It includes a total of eleven ontologies that are Extended Relation Ontology, Time Ontology, GeoSpatial Ontology, Information Entity Ontology, Agent Ontology, Quality Ontology, Artifact Ontology, Event Ontology, Units of Measure Ontology, Currency Unit Ontology, and Modal Relation Ontology. A detailed description of those ontologies is provided in [Rudnicki, 2017]. Following the selection of CCO, we move to the selection of which ontologies we shall reuse in this latter. As being said, a total of eleven ontologies were created in CCO. Amongst those ontologies, we reuse nine ontologies as follows:

- **Extended Relation Ontology:** Extends the Relation Ontology and adds required relations for building mid-level ontologies such as `has_participant`, `has_input`, and `has_output`.
- **Time Ontology:** It represents temporal intervals and relations.
- **GeoSpatial Ontology:** It represents geospatial regions and sites.
- **Information Entity Ontology:** It represents types and provenance of

5. RESONT ONTOLOGY

information.

- **Agent Ontology:** It represents agents, their qualities, and their roles.
- **Quality Ontology:** It represents the attributes of agents, artifacts, and events.
- **Artifact Ontology:** It represents artifacts, their designed qualities, functions, and models.
- **Event Ontology:** It represents events, actions, processes, and states of the world.
- **Units of Measure Ontology:** It represents the standardly employed units of measurement.

Based on this selection, we imported the selected modules and we created the common module of ResOnt. We notice that the created common module includes only the axioms obtained after the integration of the selected modules from CCO. This means that we do not add any additional axiom to this module. The aim of creating the common module is to avoid repeating the importation of the selected modules of CCO in each module of ResOnt. The common module is then specified in order to create the three different modules of ResOnt separately. Following this creation, we import the three modules and define different relations between concepts to build the complete application ontology ResOnt. Figure 5.5 illustrates different modules and the importation strategy adopted to create ResOnt ontology. In addition to the use of top and mid-level ontologies, Fernández-López *et al.* [1997] recommend the reuse of existing domain ontologies if any. In Chapter 3, an analysis of existing ontologies related to the three domains of interest was presented. A large number of ontologies were proposed in the literature in the context of emergency response and rescue operations, design of systems and interfaces, and access control and rights management. Unfortunately, the majority of those ontologies are not publicly accessible. Other ontologies that could be applied in our work such as POLARISCO [Elmhadhbi, 2020] were under construction when we started the definition of concepts in ResOnt, while others are ad-hoc ontologies oriented for specific use cases and covered particular aspects. Hence, we could not import those ontologies completely. However, we borrow some of the concepts and relations defined in these ontologies and we redefine and classify those concepts in ResOnt ontology. More details about the concepts and relations of ResOnt ontology are provided in Section 5.4.

5.3 Methodology of Ontology Development

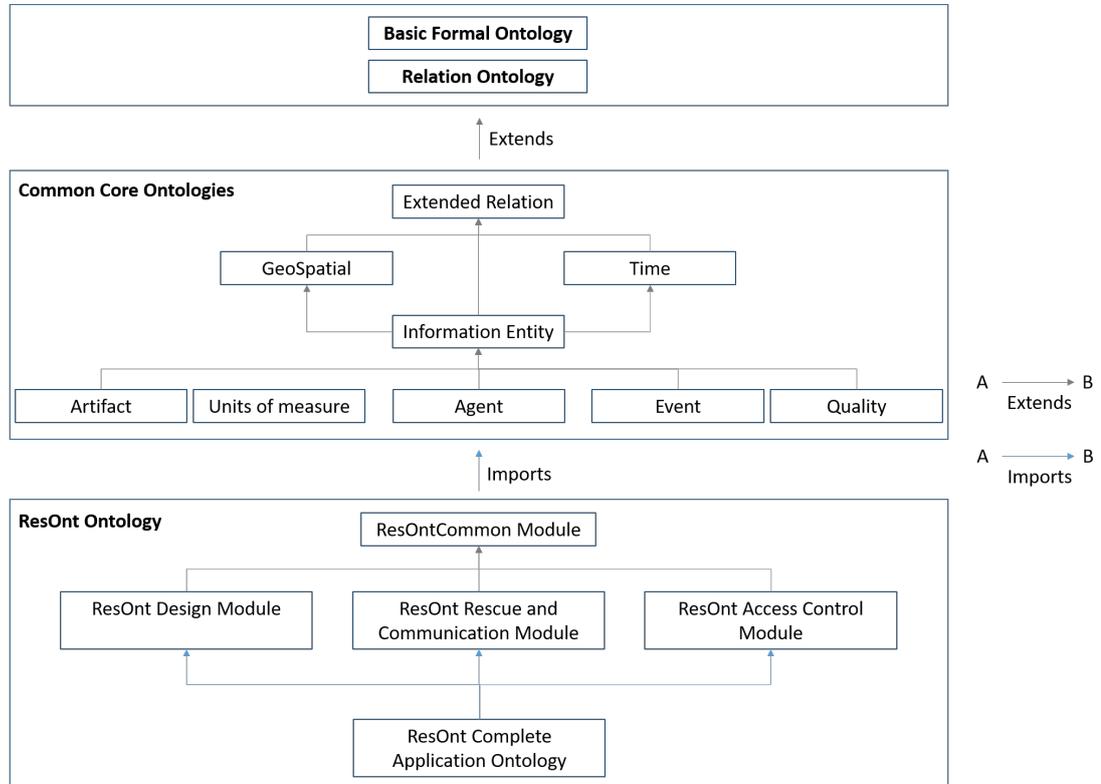


Figure 5.5: Different modules and alignment of ResOnt Ontology.

At the end of the conceptualisation phase, we obtained a conceptual ontology that includes different concepts and relations. After having presented the conceptualisation activity, let us move to the next step in the ontology development methodology. The latter step lies within the formalisation and implementation activity that is presented in the next section.

5.3.3 Formalisation and implementation

The formalisation and implementation activity consists in transforming a conceptual ontology into a formal and computational ontology [Park *et al.*, 2008]. This activity necessitates the use of a system that supports the top-level and reused ontologies chosen during the integration process [Fernández-López *et al.*, 1997]. This step results in obtaining an ontology codified in a formal language. Over the last few years, several languages for developing and querying ontologies and knowledge bases have been developed. In Chapter 3, we presented several existing languages defined in this context. Amongst these languages, the most used are

5. RESONT ONTOLOGY

RDF and OWL [Valls *et al.*, 2010; Van Harmelen *et al.*, 2008]. RDF and OWL have several similar characteristics. However, OWL is a stronger language with more computer interpretability Munir & Anjum [2018]. Hence, we proposed to encode and implement the formalised modules using the OWL-2 Language. Regarding the supporting used environment, we used Protégé software [Musen, 2015] to implement the proposed application ontology. Protégé is the most widely used software for building and maintaining ontologies. It is an open-source ontology editor and framework that incorporates a collection of tools to build ontologies. A considerable reason for using Protégé is its ease of use since it allows to define and visualise classes, relations, attributes, and rules in a simple way.

In this context, we started by reusing BFO and CCO to build the ResOnt common module. To this end, we imported BFO ontology and the selected modules of CCO and we created the common module. We would like to remember that the created common module includes only the axioms obtained after the integration CCO selected modules. Afterwards, we imported and specified ResOnt Common Module to construct the three ontology modules separately. Eventually, we imported the three different modules together and integrated them into one application ontology called “ResOnt Complete Ontology”. Figure 5.6 shows the specifications and metrics of the complete application ontology ResOnt after its implementation in Protégé. The numbers of classes, relations, and axioms of ResOnt are shown in table 5.6. As shown in Table 5.6, ResOnt includes a total of 1641 classes. In addition, it includes up to 305 object properties that refer to different relations between the ontology concepts. Following the implementation of ResOnt, we proceed to the next step that consists in evaluating the

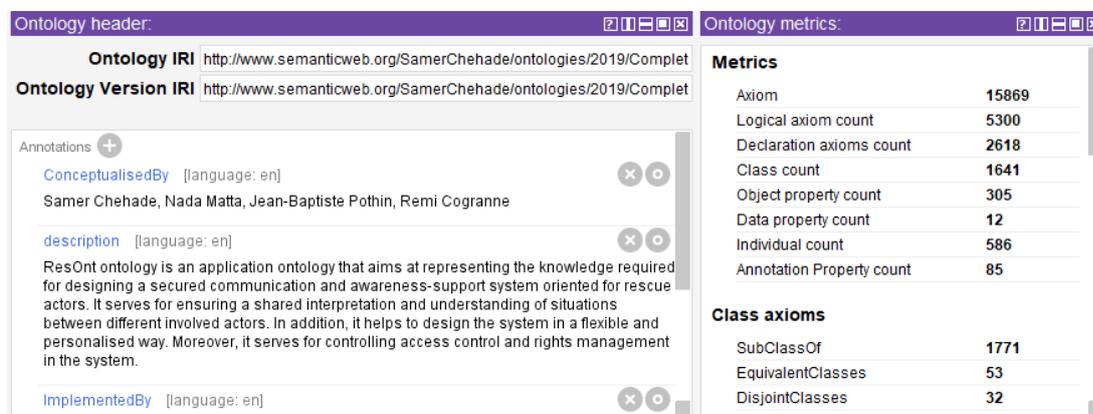


Figure 5.6: Metrics and specifications of ResOnt ontology.

Table 5.6: Classes and relations of ResOnt Ontology.

Ontology	Number of classes	Number of relations	Number of axioms
Imported Ontologies			
BFO	35	-	572
CCO	1383	249	11200
Constructed ontologies			
ResOnt Complete	223	56	4087
Total	1641	305	15859

ontology.

5.3.4 Evaluation

Several studies were conducted in the literature to analyse the ontology evaluation problems [Brank *et al.*, 2005; Hlomani & Stacey, 2014; Vrandečić, 2009]. Consequently, multiple evaluation approaches were proposed. Brank *et al.* [2005] proposed four types of ontology evaluation approaches. This classification is referred to mostly by recent research in ontology evaluations [Hlomani & Stacey, 2014]. According to [Brank *et al.*, 2005], ontology evaluation approaches can be classified into:

- **Gold Standard evaluation:** This approach consists in comparing the ontology to a “gold standard” such as another well-structured ontology. This evaluation has a considerable limitation since the gold standard itself has to be evaluated [Hlomani & Stacey, 2014].
- **Application or task-based evaluation:** This approach involves using the ontology in an application and evaluating the results. In other words, it involves assessing the effectiveness of the ontology in the context of an application. A major limitation of this approach is that what is applicable

5. RESONT ONTOLOGY

in a given context may not be applicable in another [Hlomani & Stacey, 2014].

- **Data-driven evaluation:** This approach requires comparing the ontology with existing data related to the domain of the ontology. The major limitation of this approach is that the domain knowledge is considered static while knowledge in most of the domains is dynamic [Hlomani & Stacey, 2014].
- **User-based evaluation:** This approach involves evaluating the ontology through users' experiences. The limitation of this approach results from the difficulty to establish standards about the requirements for evaluation [Hlomani & Stacey, 2014].

According to [Hlomani & Stacey, 2014], the user-based approach allows a better and more complete evaluation compared to other approaches. During this thesis, we were not able to meet a domain expert after the ontology development to evaluate it. Hence, we could not adopt this approach. However, we propose to adopt an application-based approach to evaluate ResOnt. To this end, we will instantiate the ontology and validate it through the platform and the access control policy that will be presented in Chapter 6. In this context, we will examine if the ontology can meet the fixed specifications by answering different competency questions.

5.3.5 Maintenance

The maintenance activity updates and corrects the ontology if needed [Corcho *et al.*, 2005]. This activity follows the evaluation phase and constitutes the last phase in the ontology development cycle. According to [Yildiz, Burcu, 2006], an ontology can be the subject of three kinds of changes: *Conceptual changes*, *specification changes*, and *representation changes*. Conceptual changes include possible changes in relations between concepts. Specification changes include changes related to the specifications of concepts such as the modification or addition of concept attributes. Whereas, representation changes incorporate changes in the representation of the ontology such as changing the ontology representation language [Yildiz, Burcu, 2006]. Based on its development methodology, ResOnt can be modified according to two forms of change: specification and conceptual changes. In this context, new concepts, relations, or even other ontologies can be

integrated into ResOnt. Moreover, new attributes can be added to the concepts of ResOnt. Since ResOnt is still in its first version, it has not been the subject of any modification.

After having presented the methodology adopted for constructing ResOnt ontology, we move to the description of the ontology. Hence, in the next section, we provide more details about the ontology modules and we describe the complete ResOnt ontology based on the integration of those modules.

5.4 ResOnt Ontology Description

In this section, we describe the constructed application ontology ResOnt. As mentioned above, ResOnt is an application ontology that aims at representing the knowledge required for designing a communication and awareness-support system oriented for rescue actors that guarantees the confidentiality of information. It covers distinct aspects mainly communications and practices in rescue operations, design of system and interface, and access control. In this context, ResOnt serves for ensuring a shared interpretation and understanding of situations between different involved actors. In addition, it helps to design a communication system in a flexible and personalised way that is adapted for usage. Moreover, it serves for controlling access control and rights management in the system. In 5.3.2, we presented different steps and work done to build the application ontology ResOnt following METHONTOLOGY. In addition, the reused top-level and mid-level ontologies were presented. Furthermore, an overview of ResOnt modules and the approach adopted for their construction were provided. In this section, we present different modules in detail. Hence, we start by presenting the main concepts defined in each module. Afterwards, we describe the complete application ontology ResOnt. In this context, we present the identified relations in order to obtain the complete application ontology. Moreover, we show several conceptual graphs obtained in ResOnt ontology.

5.4.1 ResOnt Rescue and Communication Module

The first module, entitled ResOnt Rescue and Communication module, is oriented for representing knowledge related to communications and practices in rescue operations. It serves for ensuring a common perception of situations between different stakeholders as well as representing and formalising different procedures

5. RESONT ONTOLOGY

and flow of information. Therefore, it constitutes a first brick toward supporting awareness in those operations. To this end, it is required to define the main concepts related to practices and interactions in those operations. In addition to the reuse of CCO, we propose to reuse several concepts defined in other existing ontologies mainly the emergency response ontology [Yu *et al.*, 2008] and the task ontology for emergency response and planning [Li *et al.*, 2008]. Those concepts are related to Tasks, resources, and events. We notice that some of those concepts were modified and reclassified to meet the CCO classification. Moreover, we have added multiple new concepts in order to cover different aspects related to practices and communications in rescue operations.

Related to awareness, which is the main interest of our work, ensuring a high level of situation awareness necessitates perceiving all elements in a situation within a volume of space and time as well as understanding their meanings and relations. Add to that, supporting communication and interactions requires identifying all the relevant information that inform on a situation. It is also necessary to identify and represent different organisations, persons, practices, and other important elements related to operations. Reusing CCO ontologies was so beneficial since they define several concepts required for representing knowledge related to communications and practices. A large number of interesting concepts were already defined and related in the selected ontologies of CCO. From those concepts, we can cite *Organization*, *Organization Member*, *Organization Member Role*, and *Communication Instrument*. However, other required concepts were not defined. A rescue operation is a response operation to a certain incident that requires the intervention of organisation members and may result in one or several victims. Based on this definition, three important concepts can be defined respectively: *Incident*, *Intervention*, and *Victim*. An *intervention* is the process of becoming intentionally involved in a difficult situation, in order to improve it or prevent it from getting worse. An *Incident* is an event that is either unpleasant or unusual. The two aforementioned concepts are classified as sub-concepts of process defined in BFO. Whereas, a *Victim* is a person harmed, injured, or killed as a result of an incident. Accordingly, we classified *Victim* as a sub-concept of the concept Person defined in the Agent Ontology of CCO. Moreover, As it has been shown in the interactions model presented in Chapter 4, each intervention is decomposed into several phases each composed of a set of sub-phases. In addition, each sub-phase starts on a precise time instance used to separate between different sub-phases. Hence, we defined three concepts respectively *Phase*, *Sub Phase*, and *Time Instance*. A *Phase* is a process boundary in a series of events

or a process of change or development. A *Sub Phase* is defined as a process boundary that is part of a longer phase. Those two concepts are classified as sub-concepts of process boundary defined in BFO. Whereas, a *Time Instance* is a temporal instant identifier that separates between two processes. Hence, *Time Instance* is classified as a sub-concept of Temporal Instant Identifier defined in the Information Entity Ontology of CCO. Moreover, each organisation member executes one or several tasks based on her/his role. Hence we reuse the concept *Task* defined in the emergency response domain ontology [Yu *et al.*, 2008]. A task is defined as an intentional act to be done or undertaken by a certain role. Accordingly, we classified task as a sub-concept of Intentional Act defined in the Event Ontology of CCO. Furthermore, we defined several tasks related to emergency response and rescue operations such as *Communication*, *Coordination*, *Rescue*, and *Evacuation* defined in [Yu *et al.*, 2008] and [Li *et al.*, 2008]. In addition, as it has been shown in the interactions model presented in Chapter 4 each of those tasks produces or uses one or several groups of information having each multiple information elements. Accordingly, we defined the concepts *Group of Information* and *Information* in this module. A group of information is defined as a generically Dependent Continuant that contains one or several information elements. It incorporates knowledge and information communicated concerning a particular task or circumstance. Regarding the concept *Information*, we defined it as a Generically Dependent Continuant that describes facts provided or learned about something or someone. Both concepts are classified as sub-concepts of Generically Dependent Continuant defined in BFO. Furthermore, each task takes place at a precise location. It is thereby essential to take different locations into consideration in the ontology. Hence, we defined the concept *Location* as a geospatial location that is the place of some process, object, or agent. Accordingly, *Location* is classified as a sub-concept of Geospatial Location defined in the Geospatial Ontology of CCO. In addition to the definition of concepts related to interactions and organisations, we have defined several concepts related to resources. For instance, we defined the concept *Material* as an artefact that can be used by organisation members during an intervention. The material can be an *Individual Protection Equipment*, a *Security Equipment*, a *Technical Equipment*, or a *Transport Equipment*. Eventually, several concepts that aim at describing distinct entities in rescue operations are defined in this module. Those latter concepts are generally classified under the concepts “realisable entities” and “quality” of BFO. For instance, each object has a *status*, *availability*, *function*,

5. RESONT ONTOLOGY

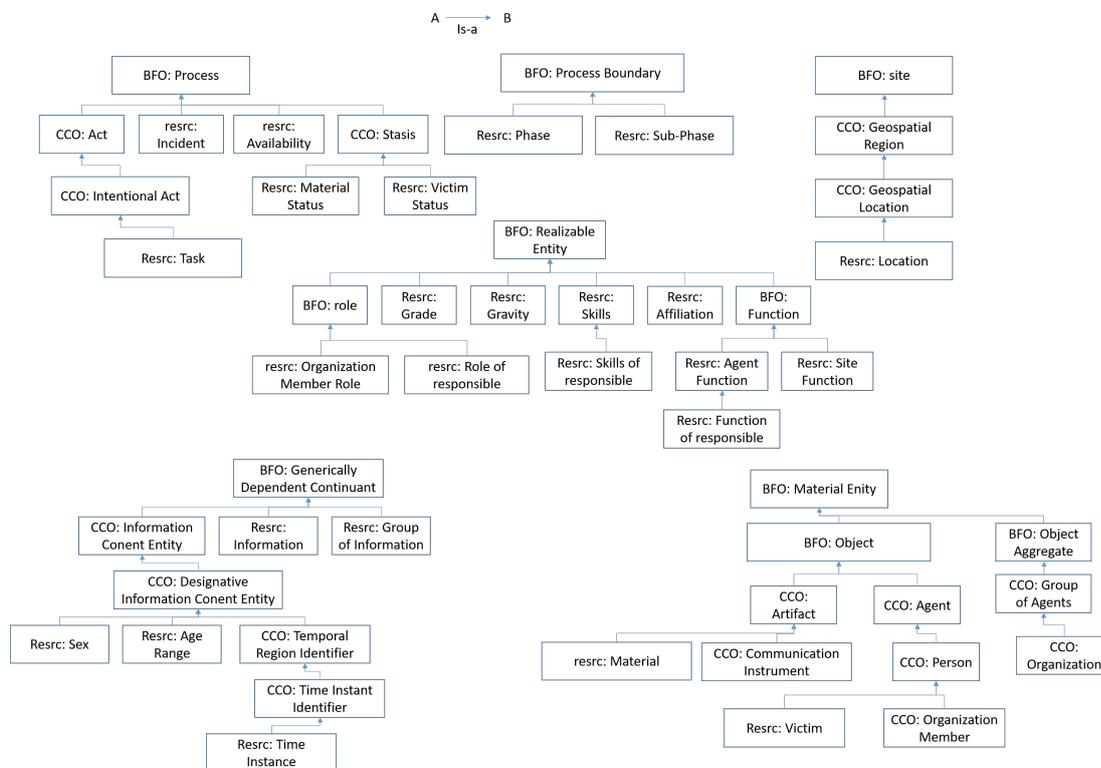


Figure 5.7: Is-a hierarchy of the ResOnt Rescue and Communication Module.

and several other characteristics. While *status* can be a *Victim status* or a *Material status*. Figure 5.7 shows the classification of concepts defined in the Rescue and Communication Module. In this figure, each concept is shown with its prefix to illustrate whether the concept is defined in BFO, in CCO, or in ResOnt. We notice that the prefix *resrc* represents the rescue and communication module in ResOnt.

5.4.2 ResOnt Design Module

The second module, so-called ResOnt Design module, incorporates knowledge required for the dynamic design and configuration of the system and interfaces in a flexible and personalised way that is adapted for usage. Related to the design of systems and interfaces, several aspects and parameters should be considered. Some of those parameters are related to the system itself such as the interface and its dimensions. Other parameters are related to the information like data type, orientation, degree of criticality, and category. Whereas, the third kind

of parameters are related to functionalities and interactions in the system. As it has been presented in Chapter 3, several ontologies were proposed related to the design of systems and interfaces. In this context, we studied the application ontology proposed in [Furtado *et al.*, 2001]. The aforementioned ontology includes several concepts related to the design such as data type, orientation, and interaction way. Hence, we reused those concepts and classified them in the ResOnt Module. The *Data type* is a particular quality of information, as defined by the values it can take. Therefore, we classified it under a concept *Types* that is a sub-concept of *Quality* defined in BFO. The *Orientation* is a quality that inheres in information and represents its direction. Whereas, the *Interaction way* is a process that describes the interaction activities between a system and its users. Accordingly, we classified the concept *Interaction way* as a sub-concept of process defined in BFO. Another interesting ontology that we have studied in this context is POLARISCO Elmhadhbi *et al.* [2019]. POLARISCO aims at enhancing semantic interoperability in emergency response operations. However, it includes important concepts related to communications and design such as the degree of criticality of information. The *degree of Criticality* is a realisable entity that represents the degree of importance of information. Indeed, it is important to take the degree of criticality of an information into consideration since it determines its position and presentation way in a certain interface. Hence we reused this concept and classified it as a sub-concept of Realizable entity defined in BFO. In addition to those concepts, we have added a new concept that represents another parameter related to information which is the field type. In this context, we defined *Field Type* as a quality that determines the nature of an information element whether it is obligatory or optional. In ResOnt Design Module, *Field Type* is classified as a sub-concepts of the concept *Types* that is a sub-concept of quality defined in BFO. Besides, we studied the Ui2Ont ontology [Paulheim & Probst, 2011]. Ui2Ont defines the semantics of the basic terms of the design and interactions domain like Interaction and User Interface Component. Moreover, it specifies and classifies the real entities that occur in the domain like types of user interface components, such as text field and button. Inspired from Ui2Ont, we defined the concept *User Interface component* and classified it as a sub-concept of *Information Bearing Artifact* defined in the Artifact Ontology of CCO. In addition, we defined two sub-concepts of *User Interface Component* that are *Informational Component* and *Media Component*. The informational component is a user interface component in which information can be fulfilled, selected, or visualised. Concerning Media Component, it consists of components

5. RESONT ONTOLOGY

that are designed to bear some media. In addition to the reused concepts, we defined several required concepts related to the system and interfaces. Concerning the parameters related to the system and its interfaces, we have identified the concept *Interface*. Each communication instrument has a specific interface, hence it is essential to differentiate between different interfaces according to the communication instrument. In this context, we defined the concept *Interface* as an information bearing artefact that is a part of a communication instrument. In addition, each interface has its dimensions. In this context, we defined the concept *Dimension* as a one dimensional extent that determines the size of an interface. We notice that *One Dimensional Extent* is defined as a sub-concept of Size Quality defined in the Quality Ontology of CCO. Moreover, in order to exchange, visualise, or fulfil information, several computational functionalities are required such as fulfilment and transmission. In this context, we defined the concept *Functionality* as a process that can be run on a computer or other communication instrument and determines the interaction way. We notice that other concepts are required related to the design such as information and communication instrument. However, those concepts were presented in ResOnt Rescue And Communication Module in 5.4.1. Figure 5.8 shows the classification of concepts defined in the Design Module. In this figure, each concept is shown with its prefix to illustrate whether the concept is defined in BFO, in CCO, or in ResOnt. We notice that the prefix *resd* represents the design module in ResOnt.

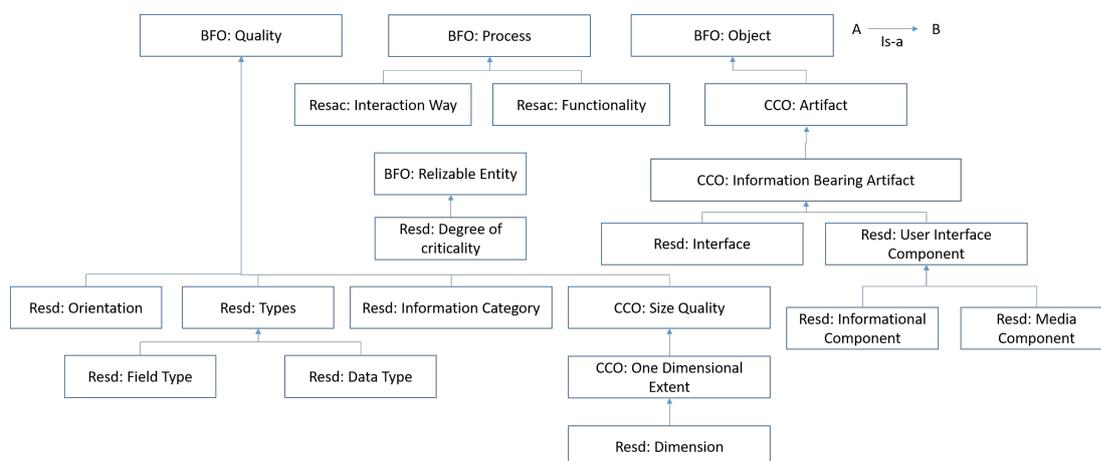


Figure 5.8: Is-a hierarchy of the ResOnt Design Module.

5.4.3 ResOnt Access Control Module

The third module, entitled ResOnt Access Control Module, is specific for representing knowledge required for guaranteeing access control and rights management in the system. As it has been discussed in Chapter 3, several access control models were developed and implemented in the literature. From those models, one can cite the Role-Based Access Control (RBAC) models [Sandhu *et al.*, 1996], the Team-Based Access Control (TMAC) model [Thomas, 1997], the Attribute-Based Access Control (ABAC) model [Yuan & Tong, 2005], as well as other models that were developed for multiple purposes [Zhou, 2008]. Moreover, several studies were conducted to develop and implement those models using ontologies. While other studies were conducted to manage access rights in real-world applications through the use of ontologies. Defining the required ontological concepts and relations in this context depends on several aspects. First, it depends on the access control model to be adopted and implemented. Each model has its specific parameters that should be represented through different concepts and relations. The selection of required concepts and relations depends also on the intent of using the ontology. Whether the ontology is intended for controlling the access, managing rights, or both of them, the ontology concepts and relations could vary. Eventually, the way of manipulating and, processing, and storing different parameters and values also affects the way of building the ontology and therefore the concepts required for this aim. In some cases, the use of ontology is limited to constitute a knowledge base. Whereas, in other cases, the ontology may serve as a knowledge and database at the same time. The aim of the Access Control Module in ResOnt is to define the access rights that an agent has on a certain group of information. Moreover, it serves as a knowledge base for determining the access type whether it is forbidden or authorised based on several parameters. Whereas, other functions required to control access the access are implemented in the final system. In this context, we do not aim to use the ontology as a database that stores dynamic information. This is due to many reasons that will be discussed in the next chapter. Accordingly, only a few concepts and relations are required. An interesting ontology related to our purpose is the ontology AMO [Buffa & Faron-Zucker, 2012]. AMO consists of a set of classes that represent different entities such as Access Type, Role, Action, Agent, Document, and Authorised Action On Resource. It also incorporates several relations and rules for managing access rights. An important concept defined in this ontology is *Action*. It defines a set of possible actions that can be carried

5. RESONT ONTOLOGY

on resources. Hence, we reused this concept and we defined it as an intentional act that can be executed on the information. *Action* is classified as a sub-concept of Intentional Act defined in Event Ontology of CCO. Another essential concept defined in AMO is *Access Type*. Indeed, there exist several types of access such as forbidden access or authorised access. In ResOnt Access control module, *Access Type* is defined as an action regulation that permits or prohibits some acts on information. Accordingly, the *Access Type* is classified as sub-concept of Action Regulation defined in the Information Entity Ontology of CCO. We notice that other concepts are required for access control such as role, task, group of information, and information. However, those concepts were presented in ResOnt Rescue And Communication Module in 5.4.1. Figure 5.9 shows the classification of concepts defined in the Access Control Module. In this figure, each concept is shown with its prefix to illustrate whether the concept is defined in BFO, in CCO, or in ResOnt. We notice that the prefix *resac* represents the access control module in ResOnt.

After having presented the main concepts defined in each module, let us move to the definition of relations between those concepts. Hence, in the next subsection, we describe the complete application ontology obtained based on defined relations between concepts.

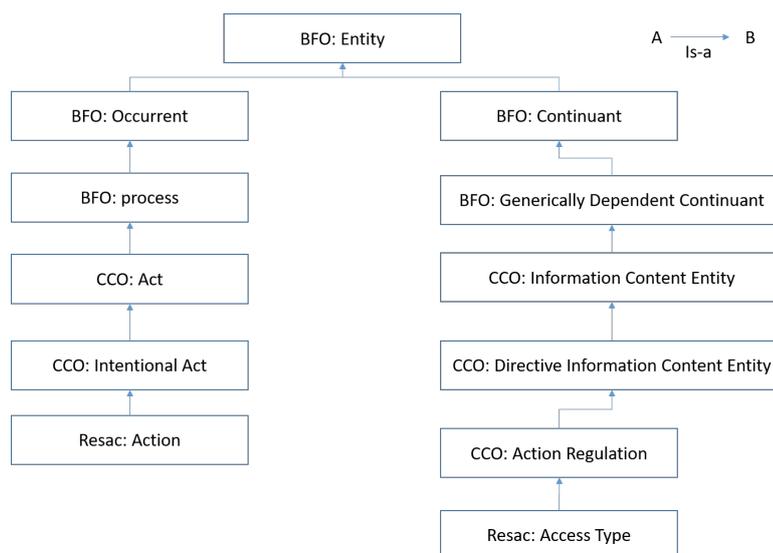


Figure 5.9: Is-a hierarchy of the ResOnt Access Control Module.

5.4.4 Complete ResOnt Ontology

Defining relations between ontological concepts is essential to obtain a complete conceptual model that can be specified based on the ontology instances. As it has been shown in 5.4.1, 5.4.2, and 5.4.3, ResOnt ontology is based on three modules: Rescue and Communication Module, Design Module, and Access Control Module. Three types of relations or properties are required to build the complete application ontology. Those relations aims at linking different concepts within and between modules. Accordingly, we classified those relations into:

- Operational properties:** They include different relations that link concepts related to communications and practices. In this context, we have reused several relations defined in CCO such as *requires*, *is cause of*, and *is affiliated with*. Moreover, we have reused the relations *has role*, *has function* from the RO ontology. Furthermore, we defined a set of new relations such as *Executes Task*, *Has Availability*, *Has Phase*, *Has Stasis*, *Has SubPhase*, *Is Associated To*, *Is Place Of*, *Occurs During*, *Starts On*, *Has Grade*, *Has Participating Role*, and *Has Skills*. Figure 5.10 shows a conceptual graph that illustrates a partial view of operational relations between different concepts. As we can see in Figure 5.10, an incident is cause of one or several victims and requires the intervention of multiple organisations. Each intervention has different phases having each one or multiple sub-phases that start on precise time instances. Moreover, each phase and sub-phase have a participating organisation role that belongs to an organisation member. This latter executes specific tasks that are associated to her/his role and take place in a certain location. Depending on the nature of the task executed, some groups of information may be used or produced. In addition, in order

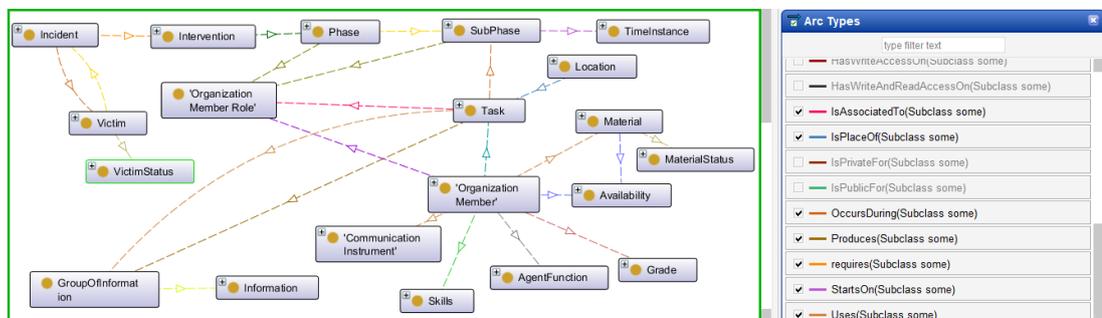


Figure 5.10: Conceptual graph related to communications and practices.

5. RESONT ONTOLOGY

to execute her/his tasks, an organisation member uses a communication instrument and some material that has a material status and availability. Besides, an organisation member has specific skills, function, and grade.

- Design properties:** They include different required relations related to the design of systems and interfaces. In this context, we have defined several design properties like *Contains*, *Defines Way*, *Has Dimension*, *Has Interface*, *Has Property*, *Is Attached to*. Some of the design properties link different concepts defined in the design module while other properties are used to link precise concepts between two modules: Rescue and Communication Module, and Design Module. Figure 5.11 illustrates a conceptual graph that shows a partial view of design properties between different concepts. As we can see in Figure 5.11, Each organisation member uses a communication instrument that has a specific interface. Having specific dimensions, an interface has different user interface components. Moreover, as mentioned above, an organisation member executes tasks that produce or use one or several groups of information and are attached to specific functionalities. Moreover, every group of information has multiple information elements. Regarding those information, they may have different properties like category, informational component, orientation, data type, field type, and degree of criticality.
- Access properties:** They include different required relations for ensuring access control and rights management. We notice that identifying relations in this context depends on the way of implementing access control and rights management mechanisms. In ResOnt, we have defined a total of six properties for this aim. Two out of those properties are required for

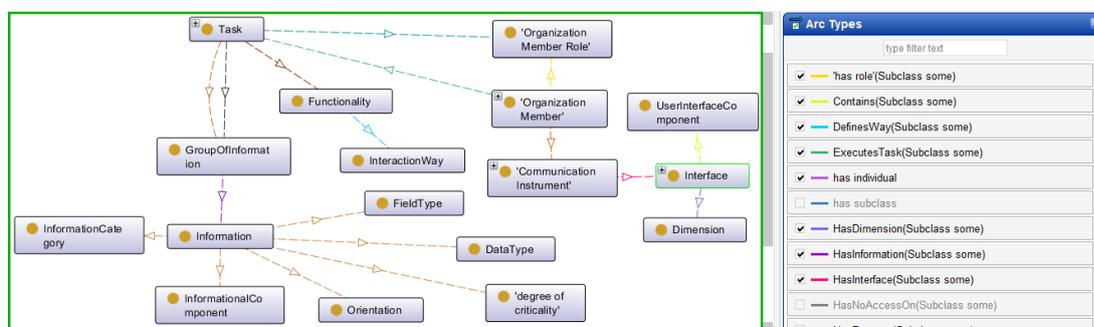


Figure 5.11: Conceptual graph related to the design of systems and interfaces.

determining the relationship between an organisation member role and a group of information in terms of privacy like *Is Public For* and *Is Private For*. Whereas four properties are needed to determine the relationship between an organisation member role and a group of information in terms of access rights such as *Has No Access On*, *Has Read Access On*, *Has Write Access On*, and *Has Write And Read Access On*. Figure 5.12 represents a conceptual graph that provides a partial view of access control properties between different concepts. As we can see in Figure 5.12, each organisation

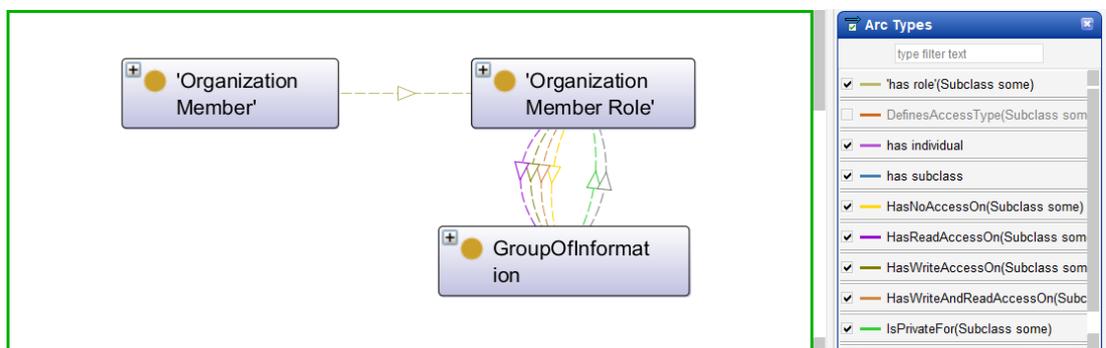


Figure 5.12: Conceptual graph related to access control and rights management.

member has an organisation member role that has some access rights on a group of information. In this context, he could have Write Access On some groups of information, Read Access On other groups of information, Write And Read Access On specific groups of information, and No Access On certain groups of information. Moreover, each group of information can be public for certain organisation roles while it could be private for other organisation member roles.

In this section, we have presented the three different modules of ResOnt ontology. Hence, we provided a detailed description of the main concepts defined in each module. Moreover, we presented a collection of reused and created relations between different concepts. Those relations resulted in the creation of a complete ontology that was also presented in this section. Tables 5.7, 5.8, and 5.9 compare ResOnt ontology to studied ontologies in three domains respectively: Communication and rescue operations, design of systems and interfaces, and access control and rights management. We notice that, most of the relations between actors in rescue operations are hierarchic relations between actors and services. However, there exist some functional relations. During the modelling step, we considered

5. RESONT ONTOLOGY

Table 5.7: Comparison of ResOnt to other existing ontologies in rescue and emergency response domain according to considered aspects.

Ontology	Persons	Roles	Organisations	Processes	Resources	Incidents	Time and Space	Communication
Emergency response	✓	✓	✓	X	✓	X	✓	X
EMERGEL	X	X	✓	X	✓	✓	✓	X
POLARISCO	✓	✓	✓	✓	✓	✓	✓	✓
EXDL-RESCUER	X	X	X	X	X	X	X	✓
PS/EM	X	X	X	X	X	X	X	✓
Emergency response domain	✓	✓	X	✓	✓	✓	X	X
IsyCri	X	X	X	✓	X	✓	X	X
BFiaO	X	X	X	X	✓	✓	X	X
BFER	X	✓	✓	X	✓	X	✓	X
CROnto	X	X	X	✓	✓	✓	X	X
EMO	X	X	✓	X	✓	X	✓	X
MOAC	X	X	X	✓	✓	✓	X	X
Task ontology for ER and planning	X	X	X	✓	X	X	X	X
ER task and data sources	X	X	✓	✓	X	✓	✓	X
ResOnt	✓	✓	✓	✓	✓	✓	✓	✓

Table 5.8: Comparison of ResOnt to other existing ontologies related to systems and interface design according to considered aspects.

Ontology	User interface components	User interface properties	Information properties	Device	Interaction	Hardware components
UIO	✓	✓	X	X	✓	X
UI2Ont	✓	✓	X	X	✓	✓
Ontology for UI design	X	X	✓	X	✓	X
AdaptUI	X	✓	X	✓	✓	✓
HCI Core Ontology	X	X	X	✓	✓	✓
ResOnt	✓	X	✓	✓	✓	X

Table 5.9: Comparison of ResOnt to other related to access control and rights management according to considered aspects.

Ontology	Roles	Organisations	Actions	Access rights	Permissions	Resources	Hierarchy
ROWLBAC Ontology	✓	X	✓	X	✓	✓	✓
Ontology for modelling RBAC model	✓	X	✓	X	✓	✓	X
Ontology for implementing RBAC mechanism	✓	✓	X	X	✓	✓	X
Access Control Ontology	X	X	✓	✓	✓	✓	X
Access Management Ontology	✓	X	✓	✓	X	✓	X
Ontology for implementing Or-BAC mechanism	✓	✓	✓	X	✓	✓	X
ResOnt	✓	✓	✓	✓	✓	✓	X

different types of relations that can exist in rescue operations. Those cover hier-

archic as well as functional relations. The hierarchic relations represent the links between different hierarchical levels. They are mainly represented in relations that exist between persons that are affiliated with the same service such as the firefighters. For instance, the relation between a CIS Operator and a sapper that are affiliated with firefighters is a hierarchic relation. Regarding the functional relations, they mainly represent relations between actors that are affiliated with distinct services. For instance, the relation between a commander of rescue operations that is affiliated with firefighters and the regulator doctor is a functional relation. We also notice that, in this work, the proposed interaction model is just an instance of a structure model applied to a specific case of organisation. However, it can be applied to other cases. Later on, other relations and instances can be added. For example, places, roles, and organisations can be modified. Similarly, the case formalised in ResOnt ontology is just an example of application that can be modified lately. Furthermore, interactions are modelled and formalised on the basis of tasks and roles. An actor can have different roles in distinct interventions. Thanks to the proposed system described in Chapter 6, an actor can reconfigure his system once his role is changed. This justifies the flexibility of our work.

5.5 Conclusions

We propose in this thesis an approach for designing a communication system that aims at supporting situation awareness in rescue operations. The second step in the proposed approach lies within the construction of an application ontology that represents the knowledge required for designing a communication system oriented for rescue actors that guarantees the confidentiality of information. Hence, as a second step, we proposed an application ontology. This ontology is referred to as ResOnt that stands for Rescue Ontology. It is mainly based on the interaction model proposed in Chapter 4. The proposed ontology consists of three modules. The first module is oriented for representing knowledge related to communications in rescue operations. It serves for ensuring a common perception of situations between different stakeholders as well as representing and formalising different procedures and flow of information. The second module incorporates the knowledge required for the dynamic design and configuration of the system and interfaces. Whereas, the third module is specific for representing knowledge required for guaranteeing access control and rights management in the

5. RESONT ONTOLOGY

system. In this chapter, we presented first the methodology adopted for developing the ontology. The aforementioned methodology consists of five activities that are Specification, Conceptualisation, Formalisation, Implementation, and Evaluation. Moreover, we presented different ontologies that we reused to develop ResOnt. We then described ResOnt ontology in detail. Hence, we presented its three modules, the concepts of each module, as well as different relations between concepts. Eventually, we presented the complete ontology obtained after the integration of those three modules.

After having modelled interactions and created an application ontology, let us move to the third and fourth steps of the approach presented in Chapter 1. The third step lies within the development of a platform oriented for rescue actors. Therefore, we design and develop a platform based on the interaction model presented in Chapter 4 and the application ontology developed in this chapter. Thanks to this platform, different involved stakeholders will be able to design the specifications and interfaces in a customised way. Moreover, they will be able to connect to an intervention and exchange information efficiently. Regarding the fourth step, it consists of guaranteeing confidential access to information through access control and rights management mechanisms. Hence, we propose an ontology-based access control policy to reinforce information confidentiality. To this end, we instantiate the proposed ontology in order to be used in the proposed platform. In the next chapter, we present the aforementioned platform, as well as the proposed access control and rights management policy.

Chapter 6

A New Secured Platform for Rescue Situation Awareness and Communications

Contents

6.1	Introduction	159
6.2	Basic Principles	160
6.3	MODES Platform Functionalities and Architecture	163
6.3.1	Main functionalities	163
6.3.2	Platform Architecture	165
6.3.3	Data flow	167
6.4	Context Identification	168
6.4.1	Context creation	169
6.4.2	Task creation	172
6.5	Dynamic and customised system and interface design	176
6.5.1	Specification configuration	178
6.5.2	Template creation	182
6.6	Communication and Access Control	187
6.6.1	User authentication	188
6.6.2	Connexion to intervention and context selection	189
6.6.3	Access Control and Rights Management	191
6.6.4	Information reception and consulting	211

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

6.6.5	Transmission of information	212
6.7	Discussion	214
6.8	Conclusions	214

6.1 Introduction

As it has been mentioned in Chapter 3, we proposed in this thesis an approach for designing a communication system that aims at supporting situation awareness in rescue operations. The aforementioned approach follows a five-step methodology illustrated in Figure 1.1. In Chapter 4, we presented the first step of the proposed approach that consists in modelling interactions and communications in these operations. Afterwards, in Chapter 5, we presented the second step that consists in developing an application ontology. As we can see in Figure 1.1, the third step in the proposed approach consists in conceiving and implementing design and communication platform in order to prove the feasibility and the relevance of our solutions. Whereas the fourth step consists in integrating confidentiality mechanisms in order to guarantee confidential access to information. As mentioned in Chapter 5, when designing a communication system oriented for rescue actors, there are several aspects and dimensions to take into consideration. First, since the system is oriented to support information exchange and awareness, it is essential to consider different practices and interactions as well as elements required for supporting awareness. In this context, it is required to determine the information required by each actor based on her/his context to enhance this awareness. Second, it is necessary to consider the dynamic design and the usage of the system in practical context and operational use cases. The system should be designed in a way that meets the practices and preferences of each participating actor. Third, since a great amount of exchanged information in rescue operations is personal and as such information is protected by laws, it is required to ensure confidential access to information in this system. Accordingly, as the third and fourth steps, we propose a design platform that allows designing the system's interfaces and specifications by the end-users themselves in a customised way. The proposed platform guarantees the confidentiality of information. It is mainly based on the interaction model presented in Chapter 4 and ResOnt ontology described in Chapter 5. Thanks to this platform, final users will be able to define the specifications related to information. In addition, each user will be able to design her/his graphical interface in a customised way based on her/his context. On the basis of those specifications and design, end-users will be able to connect to the final system in order to exchange information. In this chapter, we present first the basic principles and requirements for designing a customised communication system that guarantees the confidentiality of information. Then we describe the architecture of the proposed platform. Afterwards, we discuss

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

the main functionalities needed to meet those requirements. Moreover, the work done in the platform to ensure those functionalities will be presented.

6.2 Basic Principles

The research project presented in this thesis is part of the definition of a flexible system that improves information sharing, the first support for awareness in the domain of rescue. This system shall be designed in a way that guarantees mutual awareness between different stakeholders. Moreover, the system must gain stakeholders' acceptability by meeting their practical needs. Finally, it is of great importance that the system supports effective communications and ensures highest level of information confidentiality. For this aim, three solutions were formulated and presented in Chapter 1. Those are:

- Enhancing interactions and information exchange through a communication support system based on semantic representation and ontologies. Accordingly, the proposed system will serve for ensuring a shared representation of situations amongst involved stakeholders.
- Guaranteeing the acceptability of the system by its end-users by proposing an approach through which end-users can design the system in a customised way based on a semantic representation of knowledge. This approach will also help enhancing the flexibility and adaptability of the proposed system.
- Considering operational practices and interactions in the design of the system as well as integrating relevant confidentiality policies and mechanisms.

ResOnt Ontology, presented in Chapter 5, will mainly help to ensure a common representation of situations between different stakeholders. Furthermore, it serves as a knowledge base that represents knowledges required for designing the system and guaranteeing confidential access to information. In this chapter, we propose a platform that features an interface whose design is personalised to its end-users. Based on the interaction model and ResOnt Ontology, this platform will guarantee the confidentiality of information and respond mainly to the second and third proposed solutions. Figure 6.1 shows the basic principles of the proposed solution. As we can see in Figure 6.1, the proposed solution is mainly based on three principles blocks: Context identification, Dynamic and customised configuration and design, and, Communication and access control.

- Context Identification:** As mentioned in Chapter 4 and presented in the interaction model, different rescue actors are involved in rescue operations. Each actor has its missions and responsibilities. Moreover, each actor executes several tasks based on the one's context. An actor's context includes the intervention phase, the sub-phase, the actor's role and location, and the communication instrument used. Furthermore, each task may require or generate one or several groups of information where each group has multiple information elements. Therefore, it is necessary to determine which information are required for enhancing an actor's situation awareness based on her/his context. Accordingly, the first principle in the proposed solution consists in identifying and creating the context of usage. This step results in determining the necessary groups of information and information elements required for awareness in a certain context of usage. In this context, we propose to use ResOnt ontology as a knowledge base for determining the requirements in terms of information for different actors in distinct contexts. Indeed, ResOnt is mainly based on the interaction model proposed in Chapter 4. Therefore, using ResOnt in this stage can be very beneficial to determine the context elements as well as the requirements in terms of information in each context.
- Dynamic configuration and customised design:** Several studies report a low adoption of communication systems in rescue operations as well as negative feedbacks from actors to such systems [Elmasllari, 2019]. The

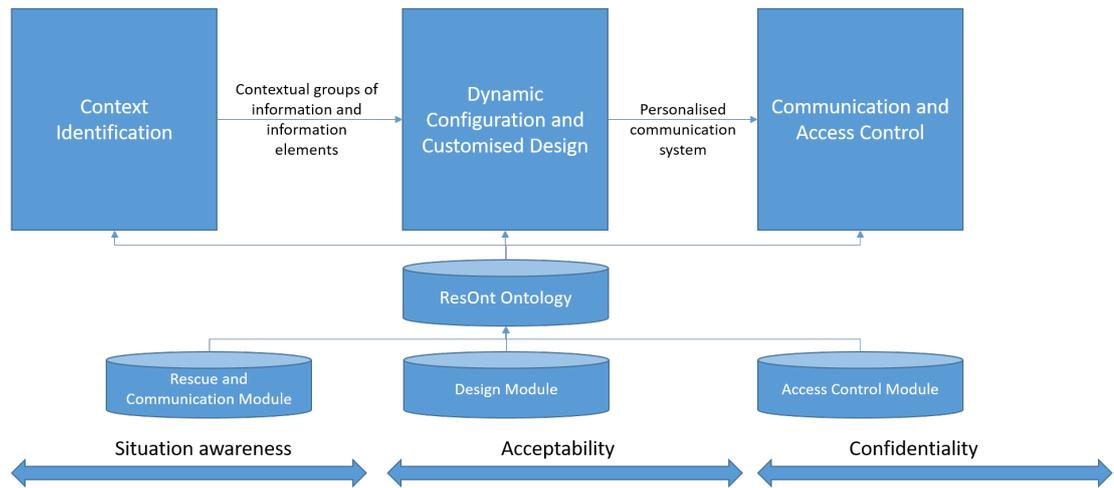


Figure 6.1: Basic principles of the proposed solution.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

current needs of stakeholders, roughly speaking, are not fully satisfied by the offered systems. Observing this circumstance through a design focal point, we notice that such issues ordinarily originate from the use of irrelevant design techniques as well as inadequate approaches to collect and understand user' requirements. Indeed, each user has specific requirements based on her/his context and preferences. Eventually, communication systems oriented for rescue operations are subjects to continuous modification. For instance, domain concepts such as the organisation member roles could be changed with time. Therefore, the system should be flexible to any modification upon requirements. Moreover, it is strongly required to allow the end-users to define the system specifications and design the graphical interfaces in a dynamic and personalised way. In this context, those users should be able to configure the system specifications. We notice that system specifications incorporates different parameters related to information such as the data type, the informational component, field type, and other parameters. Moreover, each user must be able to design the system's graphical interfaces according to the created contexts. This step results in a personalised and flexible communication system that will gain the acceptability of its end-users. To this end, ResOnt ontology can serve as a relevant knowledge base for ensuring this flexibility. Indeed, an ontology can be simply updated when the design requires the modification or consideration of new information and properties. In addition, ResOnt serves for incorporating the concepts required for the design of interfaces such as information, communication instrument, and user interface component, as well as relations between those concepts.

- **Communication and Access Control:** In order to support awareness, rescue actors must be able to communicate effectively by transmitting, receiving, and visualising information based on their contexts. However, a great amount of exchanged information in rescue operations is personal and sensitive information. Of course, as confidential information is shared between a group of within or across different organisations, enforceable protection and privacy regulation over information access is a crucial feature. In this context, it is strongly required to forbid any external access to this information. Moreover, based on their roles and tasks, participating actors should have different access rights to information. For instance, a group leader can read or modify a medical record whereas a CTA Operator is

not allowed to access medical information about victims. Hence, access to information should be controlled and restricted to the allowed persons. Access control and rights management mechanisms are suitable for maintaining access to information and monitoring the actions of legitimate users by mediating any attempt by the user to access a resource within the system [Abomhara *et al.*, 2016]. Hence, the third principle consists in ensuring the confidentiality of information by integrating access control and rights management mechanisms in the communication system. In this context, ResOnt serves as a relevant source for determining access rights since different roles and tasks are defined in this ontology. Moreover, it incorporates different concepts and properties used in access control like action, access type, access rights, and organization member role. The result of this step is a communication system that allows effective communication and guarantees the confidentiality of information in rescue operations.

6.3 MODES Platform Functionalities and Architecture

Based on the basic principles, several functionalities must be ensured in the proposed solution. In this next section, we present an overview of those functionalities. Moreover, we describe the general architecture of the proposed solution.

6.3.1 Main functionalities

Thanks to this platform, we aim to support the users in configuring the communication system's specifications and designing interfaces. In section 6.2, we presented the basic principles of the proposed solution respectively: Context identification, Dynamic and customised configuration and design, and Access control and rights management. In order to respect those principles, the proposed platform must provide several functionalities to its end-users. The main functionalities are: (1) Creation of context; (2) Configuration of context elements; (3) Checking what are the tasks associated with the user depending on her/his context; (4) Checking what are the groups of information and thus information that is available to a user in a context; (5) Configuring the system specifications

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

and information properties based on a set of proposed properties and possible values; (6) Creating personalised templates related to contexts and users identities; (7) Adding required media components to the user interfaces; (8) Positioning of different informational components and media components in created templates; (9) Connecting to the final system after its design; (10) Creating, transmitting, receiving, and visualising information while respecting the access control policy. As mentioned in section 6.2, the proposed solution is mainly based on ResOnt ontology. In Chapter 5, we presented several conceptual models based on relations between different concepts defined in the ontology. After having created the conceptual models, it is necessary to instantiate this ontology. Moreover, it is essential to identify different relations between those instances. The importance of this instantiation and relations is to be able to create a complete knowledge base through which that serves for making the required inferences. For instance, based on those instances, possible values can be proposed to the user during the design phase as well during the use of the communication system. Accordingly, we instantiate concepts related to interactions and we define relations between them based on the interaction model presented in Chapter 4. Moreover, we instantiate concepts related to interface design by assigning a set of possible values to each concept. In addition, concepts required for access control are instantiated and related in order to employ the access control and rights management policy. At the end of this step, we obtain an ontological knowledge base that we can be queried to check the tasks associated with each user according to her/his context. Additionally, each user will be able to check what the requirements for each task are in terms of groups of information and information. Moreover, it is likely to get the possible values for each one of the properties defined for information as well as other concepts related to the interface design. Furthermore, we are able to define rules required for the access control and rights management policy. In addition, it is possible to extract the access type based on the access control policy. These queries can be executed by using the SPARQL language [Harris *et al.*, 2013]. The importance of these capabilities is that they are essential for the functionality of the proposed platform and the access control mechanism. More details and examples about those functionalities and the ontology instances will be presented in sections 6.4, 6.5 and 6.6 respectively.

6.3.2 Platform Architecture

As it has been presented in 6.3.1, different functionalities are required in the proposed solution in order to meet the basic principles. On the one hand, some functionalities require the use of a knowledge base. On the other hand, other functionalities rely on using a database for storing dynamic information such as those exchanged in the final system or user credentials required for authenticating different users. In order to manipulate the different functionalities, we proposed to design the platform as shown in Figure 6.2, which shows the general architecture and main components of the proposed platform. As we can see in Figure 6.2, the platform includes a front-end, a back-end, a database, and, a Knowledge base with an inference engine.

- Front-end:** It consists of the user interface and the code behind through which end-users are supposed to interact with the platform. The main objective of the front-end is to manage the presentation of information and components to the user. Moreover, it serves for transmitting HTTP requests from clients to the Back-end and returning results on the way back. To develop the front-end several languages could be used such as ReactJS

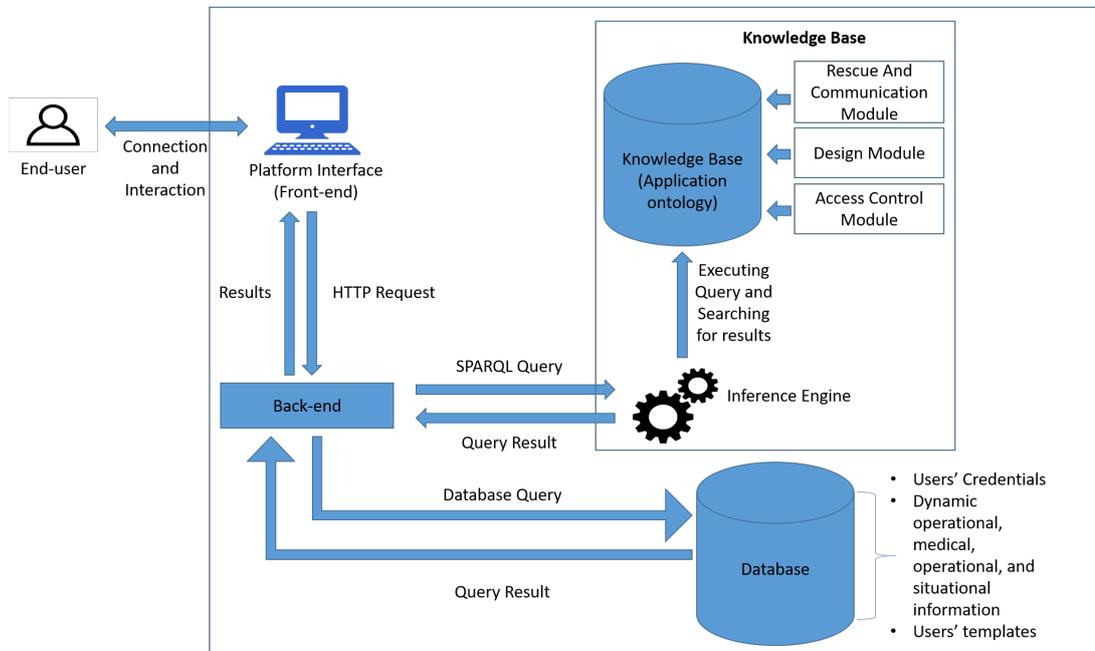


Figure 6.2: General Architecture of the proposed platform.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

[Fedosejev, 2015].

- **Knowledge base and inference engine:** As mentioned previously, the proposed solution is based on the use of the application ontology ResOnt. In this context, it is essential to integrate the ontology knowledge base in the architecture. This knowledge base will serve for storing the knowledge related to communications and interactions, as well as the knowledge required for the design of systems and controlling access. Moreover, in order to make the required inferences, the architecture must include an inference engine. This latter will serve for searching and retrieving the relevant results from the knowledge base on the basis of user's requests. Jena Fuseki server can be used for instance for storing the knowledge base and executing the required inferences [Jena, 2014].
- **Database:** Several functionalities of the proposed solution requires the use of a database together with the ontology. Indeed, the ontology serves for storing static knowledge required in the proposed solution. In addition, it could be used for storing a set of possible values required in the solution. Those values are stored as concepts' instances in the ontology. However, other types of data require the use of a database. The authentication of users, the storage of dynamic information represented by situational and medical information, as well as the storage of configured values, contexts, and templates, imply the employment of a database in the proposed solution. One main disadvantage of using knowledge bases as databases is the limitation of knowledge bases in case of a large volume of data. Accordingly, we used a database for storing personal and dynamic data exchanged in rescue operations. Furthermore, this database will serve for storing different contexts and templates created during the design of the system.
- **Back-end:** The back-end represents the platform component that handles different functions. It manages different interactions with the server. Moreover, it includes different SPARQL queries and database queries required for storing and retrieving knowledge and data from the knowledge base and database respectively. It can be based on the model of REST API. As we can see in Figure 6.2, each client request is transmitted from the front-end to the back-end. Accordingly, the back-end will execute the corresponding SPARQL or database query to the knowledge base or database. On the way back, the results are returned to the back-end that returns them to

the end-user through the platform interface. The technology used in the back-end can be Strapi for example.

6.3.3 Data flow

As we can see in Figure 6.2, there exist two main cases of operation. The first case consists in extracting knowledge and values from the knowledge base and returning the results back to the user. In this case, an HTTP request is transmitted from the front-end to the back-end that will handle the request and execute the corresponding SPARQL query to the knowledge base. Since our aim is for using the ontology is limited to the extraction of information, the HTTP request in this first case is always a GET request. Hence, the back-end will handle this request and executes a corresponding SPARQL query to the knowledge base. Based on the executed query, The inference engine will handle it, extract the results, and return them to the back-end. Those results are then parsed in the back-end. Eventually, those results are returned to the front-end to be presented to the user.

Regarding the second case of operation, it lies within querying the database in order to retrieve, modify, delete, or create new data. In this context, the HTTP request could have four different types PUT, DELETE, GET, and POST that corresponds to updating data, deleting data, retrieving data, and creating data respectively. Regardless of the type of HTTP request, each request is transmitted from the front-end to the back-end that handles it and executes the corresponding query on the database. An HTTP request is transmitted from the front-end to the back-end. Hence, the back-end will handle this request and executes a corresponding database query to the database. Based on the executed query, the database will handle it and return corresponding results to the back-end. Those results are then handled by the back-end and returned to the front-end to be presented to the user.

After having presented the basic principles, an overview of the main functionalities and the platform architecture in detail, we move to the description of those functionalities. Hence, in sections 6.4, 6.5, and 6.6, we present more details of the required and developed functionalities and mechanisms in order to respond to those principles.

6.4 Context Identification

As mentioned in section 6.2, the first principle of the proposed solution consists in context identification. Context identification represents the first main activity to be achieved by the system end-users. It serves mainly for determining the information required by each user based on his context. We recall that a context includes the **Phase** and **Sub-phase** of the intervention. Those two parameters represent determined intervals of time during an intervention. A context also includes the **Location**. Rescue actors execute several tasks where each task has a specific location. Moreover, the user's context incorporates her/his **Role**, as well as the **Communication instrument** used. Participating actors in rescue operations have different contexts. For instance, a commander that leads a rescue operation does not have the same role and tasks as a CTA Operator. In addition, they exist in distinct locations, use different communication instruments, and does not necessarily participate in the same intervention phases and sub-phases. Context's differences are not limited to those between different users. Indeed, each actor can have different contexts during a single intervention. For example, one actor could participate in different phases and exist in various locations. Therefore, it is essential to identify different contexts in order to determine the requirements in terms of information. Context identification is an activity assigned to each end-user who aims at designing her/his proper graphical interface. Figure 6.3 shows a use case diagram for context identification. As we can see in Figure 6.3, the context identification activity consists of two sub-activities that

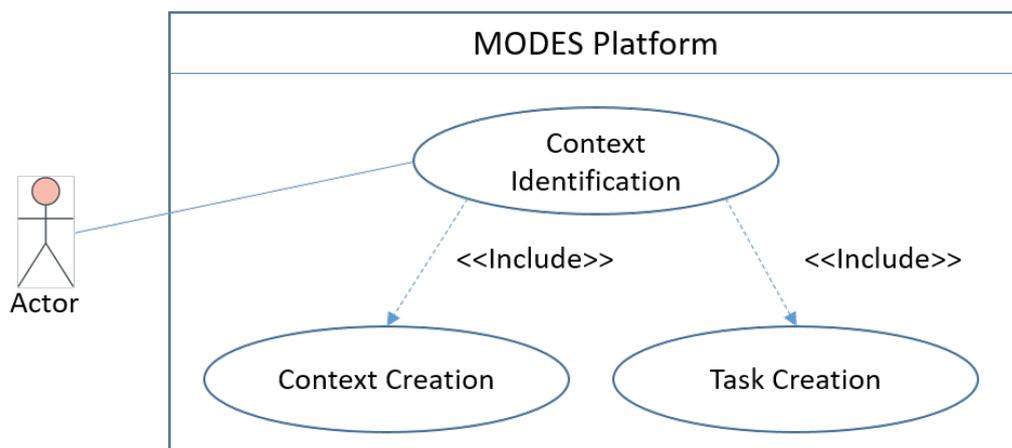


Figure 6.3: Use case diagram for context identification.

are: (1) Context creation; and (2) Task creation. Context creation is the procedure of generating specific contexts by assigning specific values to each one of the context elements presented above. In this case, some parameters should be determined automatically in the proposed solution such as the user role and id based on the authentication process. On the opposite, other context elements are configured by the end-user himself. In order to ease the end-users' tasks in the context creation activity, they must be able to configure those elements based on a set of proposed values. Hence, we proposed to define those values as concepts' instances in ResOnt ontology. Regarding the task creation, this activity consists in checking what are the tasks associated with the user depending on her/his context, checking what are the groups of information and thus information that is produced or required for achieving each task in the context, deleting a group of information or information from a specific task, determining the groups of information and information required in a context after the configuration of different tasks.

In order to give the end-users access to those activities, the first two functionalities required in the solution are:

- Context creation
- Task creation

6.4.1 Context creation

As aforementioned in the previous paragraph, in this step, the user must be able to create a context by configuring different context elements that are: Phase, sub-phase, role, location, and communication instrument. Several solutions that take the user's context into consideration were developed. However, in our best knowledge, only few solutions allow the end-users to identify and configure their own contexts. Thanks to the context creation functionality, the proposed solution will allow end-users creating their contexts and support them during this creation on the basis of their practical operations. The created contexts are then related to the user and stored in the database for further retrieval. Figure 6.4 illustrates a sequence diagram for the context creation activity. As shown in Figure 6.4, when the user starts the context creation, her/his role is extracted automatically based on the authentication phase (Cf. Section 6.6.1). A request is then transmitted from the front-end to the back-end in order to get the possible phases based on the user's role. Therefore, a corresponding SPARQL query will be executed on the

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

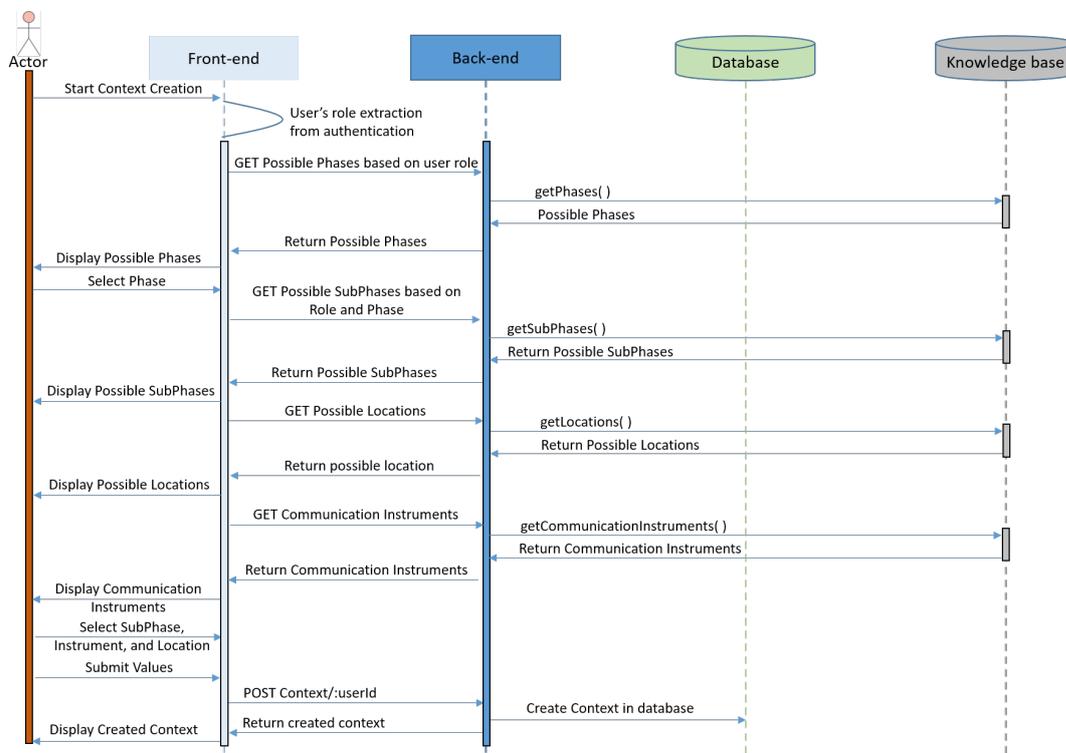
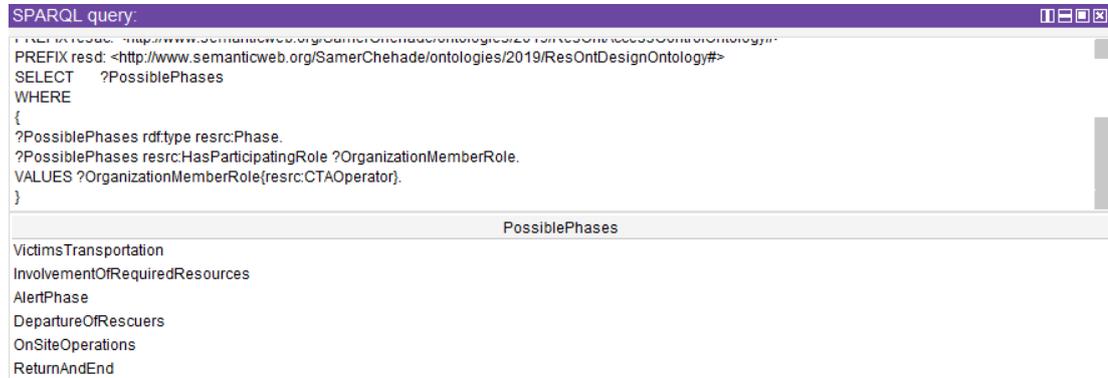


Figure 6.4: Sequence diagram for context creation.

knowledge base and different possible phases that the user's role participates in are returned back to the user passing through the back and front-end. Figure 6.5 shows a SPARQL query that retrieves different phases having *CTA Operator* as a participating role. As we can see in Figure 6.5, a *CTA Operator* participates in different intervention phases that are: Alert Phase, Involvement of required resources, Departure of rescuers, On-site operations, Victims transportation, and Return and end. Hence, the user will select a specific phase through the set of proposed phases. Following this selection, the user must be able to select a specific sub-phase. Accordingly, after the phase selection, another request is transmitted from the front-end to the back-end in order to retrieve the possible sub-phases from the knowledge base. We notice that the possible sub-phases should be extracted on the basis of the selected phase and the user's role. The importance of this dependence is to orientate the user's during the context creation. Hence, a corresponding SPARQL query will be executed on the knowledge base and appropriate sub-phases will be retrieved and returned to the front-end. At the same time, two other requests are generated from the front-end and transmitted



The screenshot shows a SPARQL query window with the following content:

```

SPARQL query:
PREFIX resdc: <http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#>
SELECT ?PossiblePhases
WHERE
{
?PossiblePhases rdf:type resdc:Phase.
?PossiblePhases resdc:HasParticipatingRole ?OrganizationMemberRole.
VALUES ?OrganizationMemberRole{resdc:CTAOperator}.
}

```

The results table is titled "PossiblePhases" and contains the following entries:

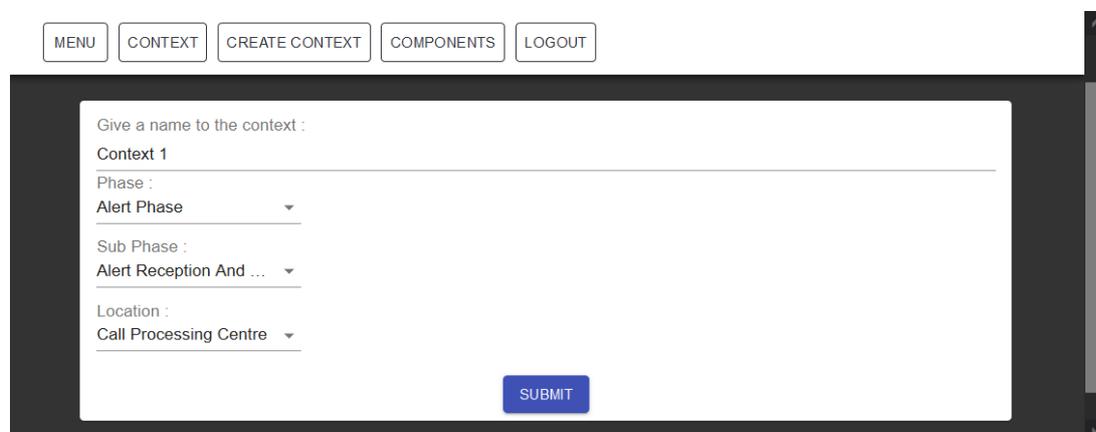
PossiblePhases
VictimsTransportation
InvolvementOfRequiredResources
AlertPhase
DepartureOfRescuers
OnSiteOperations
ReturnAndEnd

Figure 6.5: SPARQL Query for retrieving different phases based on a specific organisation member role.

to the back-end. Those latter serve for retrieving different values of Location and Communication Instrument. Accordingly, different possible locations and communication instruments will be also retrieved and returned to the user. This latter will then select three specific values for sub-phase, location, and communication instrument on the basis of the returned values. When those values are submitted, the front-end will transmit a POST request containing the user id and the selected values to the back end in order to create and store the context in the database. The context will be then created and displayed to the user through the graphical interface.

As mentioned in 6.3.1, in order to support the user’s during the context creation, and to ensure the required functionality by responding to the different queries, it is essential to instantiate the ontology and relate those instances. Hence, we have instantiated different concepts In ResOnt Ontology that represent context elements and related them based on the interaction model presented in Chapter 4. For instance, a communication instrument can be a Desktop, Laptop, Tablet, or Smartphone. Figures 6.6 and 6.7 illustrate an example of a context creation by an end-user having the role of CTA Operator. As we can see in Figure 6.6, in this example, we configured the context by selecting the “Alert Phase” as the intervention phase, “Alert reception and processing” as sub-phase, and “Call Processing Centre” as Location. Regarding the communication device, based on the interaction model, we have selected “Desktop” as shown in Figure 6.7. After having created a context, the user will be redirected to the task creation section as shown in Figure 6.8. As we can see in Figure 6.8, in this section, the

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

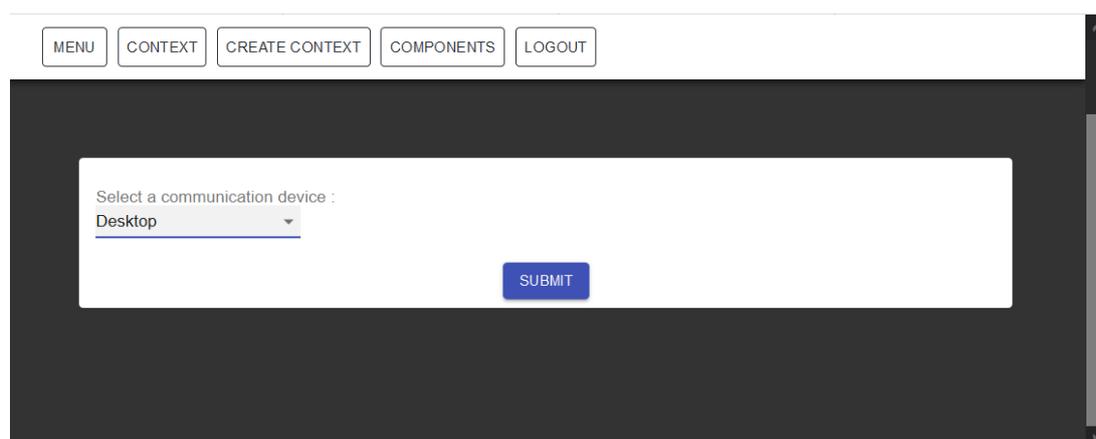


The screenshot shows a web interface with a navigation bar at the top containing buttons for 'MENU', 'CONTEXT', 'CREATE CONTEXT', 'COMPONENTS', and 'LOGOUT'. Below the navigation bar is a form titled 'Give a name to the context :'. The form contains the following fields:

- Context 1** (text input)
- Phase :** Alert Phase (dropdown menu)
- Sub Phase :** Alert Reception And ... (dropdown menu)
- Location :** Call Processing Centre (dropdown menu)

A blue 'SUBMIT' button is located at the bottom right of the form.

Figure 6.6: Selection of phase, sub-phase, and location in MODES platform.



The screenshot shows a web interface with a navigation bar at the top containing buttons for 'MENU', 'CONTEXT', 'CREATE CONTEXT', 'COMPONENTS', and 'LOGOUT'. Below the navigation bar is a form titled 'Select a communication device :'. The form contains the following field:

- Desktop** (dropdown menu)

A blue 'SUBMIT' button is located at the bottom right of the form.

Figure 6.7: Selection of communication instrument in MODES platform.

user will have an overview of the context created as well as the interface required for creating tasks.

6.4.2 Task creation

After having created the context, the end-user has to create different tasks that are associated with her/his role in the given context. Based on this creation, the end-user will get an overview of different groups of information produced or required by each task. Moreover, following the creation of different tasks in a given context, it is likely possible to determine the necessary groups of information and information elements in the context. The task creation activity results

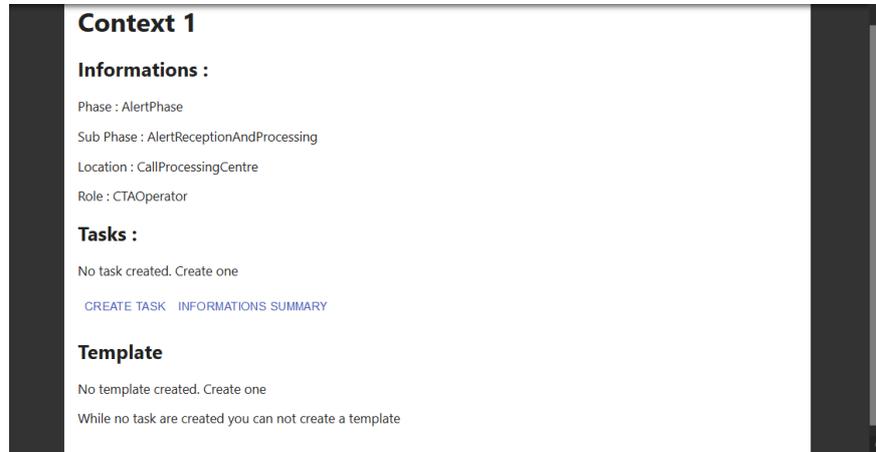


Figure 6.8: Task creation section in MODES platform.

in determining the necessary groups of information and information elements required by a user. Moreover, it allows end-users configuring different tasks on the basis of the practical operations. Hence, thanks to this functionality, the proposed solution helps ensuring effective communication and situation awareness amongst different actors. We notice that, in a given context, some tasks produce or require identical groups of information. Hence, it is essential to display those groups only one time to the user to avoid repetition. Figure 6.9 illustrates a sequence diagram for the task creation activity. As shown in Figure 6.9, when the user starts the task creation, a request is transmitted from the front-end to the back-end in order to get the possible tasks associated with the user's role based on the context created. Therefore, a corresponding SPARQL query will be executed on the knowledge base and different tasks are returned back to the user passing through the back and front-end. Hence, the user will select each task from the return list in order to check its requirements in terms of groups of information. On the basis of the selected task, a new request is transmitted from the front-end to the back-end in order to retrieve the groups of information and corresponding information. Hence, a first SPARQL query will be executed on the knowledge base and appropriate groups of information will be retrieved. Moreover, for each group of information returned, another SPARQL query is executed on the knowledge base to extract the related information. Once retrieved, those groups of information and information are returned to the front-end to be displayed to the user through the graphical interface. Therefore, the end-user will be able to delete any group of information or information element from the task

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

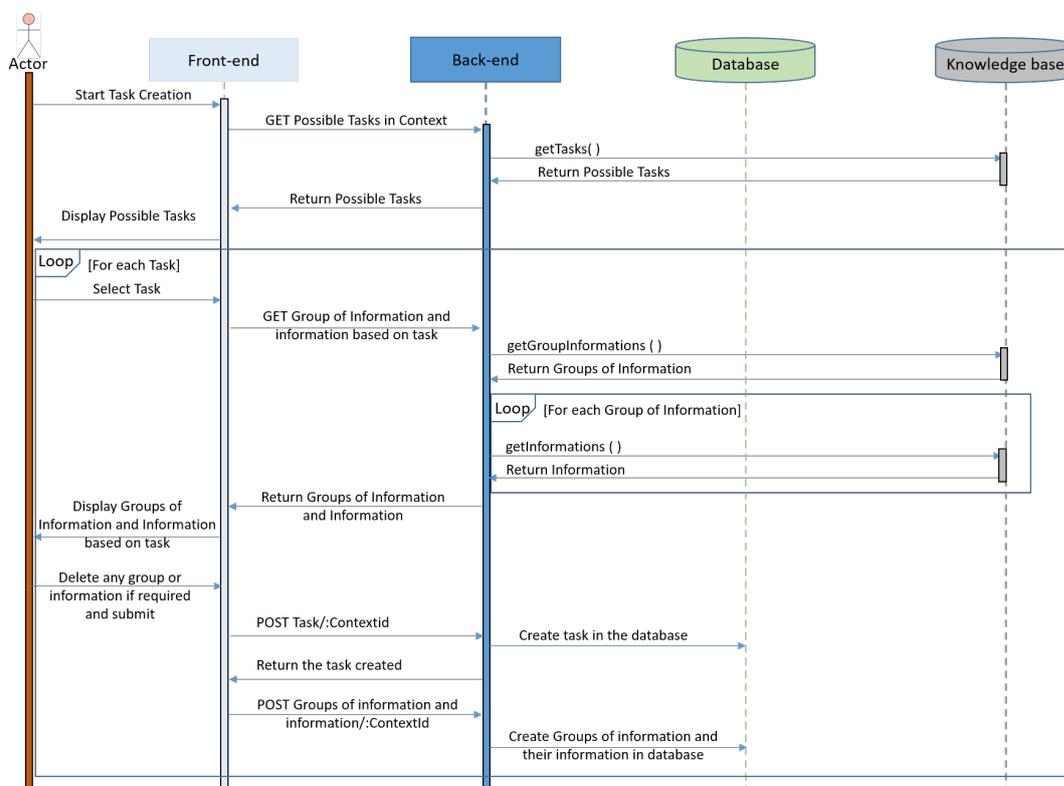


Figure 6.9: Sequence diagram for task creation.

if required and submits her/his choices. When the user's choices are submitted, the front-end will transmit a POST request to the back-end containing the context id and the task in order to create this latter in the database. The task will be then created. In addition, another POST request containing the context id as well as the groups of information and information is transmitted to the back end in order to create and store those latter in the database. Accordingly, if the groups of information and information do not already exist in the given context in the database, those groups of information and information elements will be created in the database. However, if those groups of information and information elements are already created, the creation step in the database is not executed. The importance of this test is to avoid the creation of groups of information and information several times in a given context in the database.

Similarly to the context creation activity, in order to ensure the required functionalities in the task creation activity, it is necessary to instantiate the ontology and relate those instances. For instance, different tasks, groups of information, and

6.4 Context Identification

information must be defined in the knowledge base. Hence, we have instantiated different concepts that represent tasks, groups of information, and information and related them. Moreover, each task's instance was associated with a specific organisation member role, and related to specific sub-phase and location based on the interaction model presented in Chapter 4. Figures 6.10 and 6.11 show an example of task creation by an end-user having the role of CTA Operator based on the context created in Figures 6.6 and 6.7. As we can see in Figure 6.10,

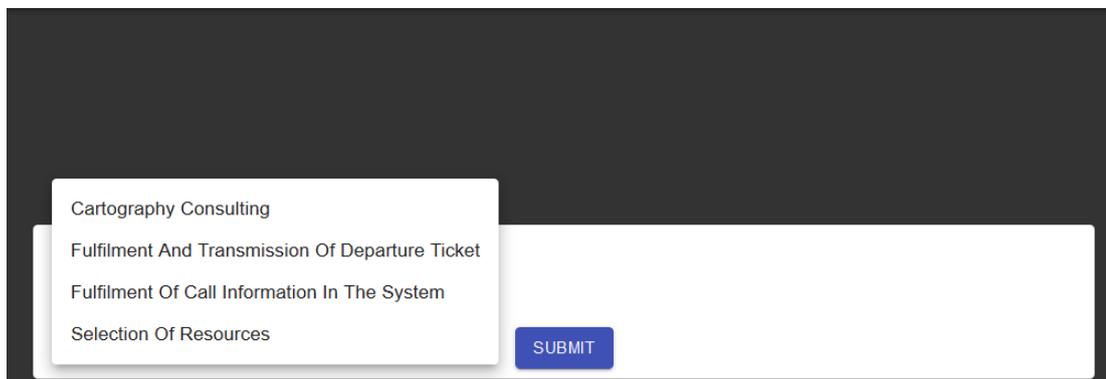


Figure 6.10: Creation of task in a given context in MODES platform.

Group Info

Centres Cartography ⊖

Property : Uses

Informations	
Address	⊖
Distance	⊖
Name	⊖

Material Cartography ⊖

Property : Uses

Informations	
Material	⊖
Availability	⊖

Figure 6.11: Configuration of a created task in MODES platform.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

on the basis of the created context, the CTA Operator has four different tasks. Hence, we have selected the “Cartography Consulting” task as an example in order to configure it as shown in Figure 6.11.

After having created different tasks in the context, the user will be able to check a summary of groups of information and information in the context as illustrated in Figure 6.12. After having presented the first principle in detail, its related activities, as well as the required functionalities for this aim, let us move to the second principle.

6.5 Dynamic and customised system and interface design

As mentioned in section 6.2, the second principle of the proposed solution lies within the dynamic configuration and customised design of the system. This latter represents the second main activity to be achieved by the system end-users. It serves mainly for defining the system’s specifications in a flexible way. Indeed, communication systems oriented for rescue operations are subjects to continuous modification. Such modifications mainly result from required changes in the

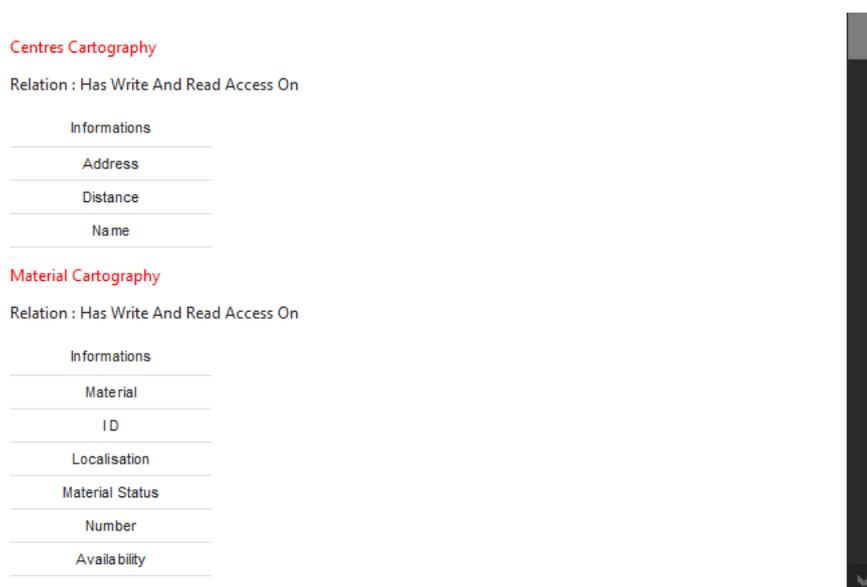


Figure 6.12: Summary of contextual groups of information and information elements.

6.5 Dynamic and customised system and interface design

system's specifications. Therefore, the system should be flexible to any modification upon requirements. Moreover, the system's users should have the ability to configure those specifications by themselves in a way that meets their needs. On the other hand, multiple end-users with different requirements and preferences are supposed to use the communication system. For instance, intervention team members on the intervention site require the integration of maps in the graphical interface whereas medical doctors in hospitalisation centres do not have this requirement. Those differences in preferences are not limited to those between different users. Indeed, each actor can have different preferences based on her/his context. For instance, a single actor may require differences in information positioning on the graphical interface based on the context of use. Therefore, it is essential to give the end-users the ability to design different graphical interfaces on the basis of their preferences and the context of use. Figure 6.13 shows a use case diagram for dynamic configuration and customised design. As we can see in Figure 6.13, the dynamic configuration and customised design activity consists of two sub-activities that are: (1) Specification configuration; and (2) Template creation. Specification configuration is the procedure of configuring several parameters by assigning specific values to each one of those parameters. We recall that the system's specifications incorporate different properties related to information that are data type, informational component, field type, degree of criticality, information category, and orientation. In order to guarantee the functionality and interoperability of the communication system, it is essential to unify the system's specifications between different users. Accordingly, this activ-

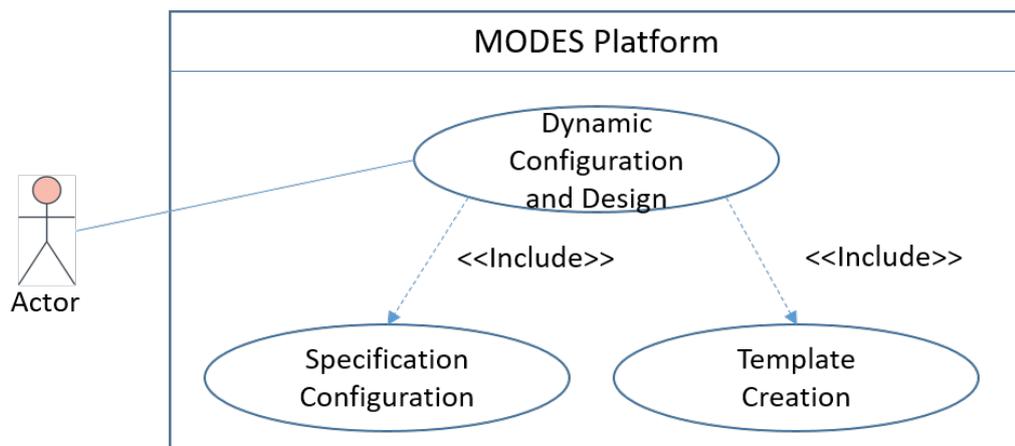


Figure 6.13: Use case diagram for dynamic configuration and customised design.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

ity should be achieved mainly by the system's administrators. For simplifying the administrator's tasks in the specification configuration activity, they must be able to configure those parameters based on a set of proposed values. Hence, we proposed to define those values as concepts' instances in the knowledge base. Moreover, each value should have pre-implemented functions and integrated into the system. Regarding the templates creation, this activity consists in creating and designing different templates by: (1) Visualising different contextual groups of information and information elements in specific informational components based on the specifications configuration activity; (2) Integrating required media components in the templates; and (3) Positioning different informational and media components on those templates. This step results in multiple personalised templates where each template is specific to the user who creates it and to a specific context of usage.

In order to give the end-users access to those activities, two functionalities required in the solution are:

- Specification configuration
- Template creation

6.5.1 Specification configuration

When developing communication systems, dynamic configuration of their specifications is barely considered. In this context, most of the existing solutions are specified and pre-configured by the systems' providers. This may cause several problems in case of any required modification in those specifications. Accordingly, thanks to the specification configuration functionality, we aim through the proposed solution to propose a flexible system that can be configured by its administrators in a dynamic way. As stated in the previous paragraph, in this step, the system's administrators must be able to configure different specifications by assigning specific values to several parameters. The configured specifications are then stored in the database for further retrieval. Moreover, different functions should be already implemented and integrated into the development phase to be executed based on those specifications. Figure 6.14 illustrates a sequence diagram for the specifications configuration activity. As shown in Figure 6.14, when the system's administrator starts the configuration of specifications, a request is transmitted from the front-end to the back-end in order to get all the groups of information. The aim of retrieving the groups of information is that several

6.5 Dynamic and customised system and interface design

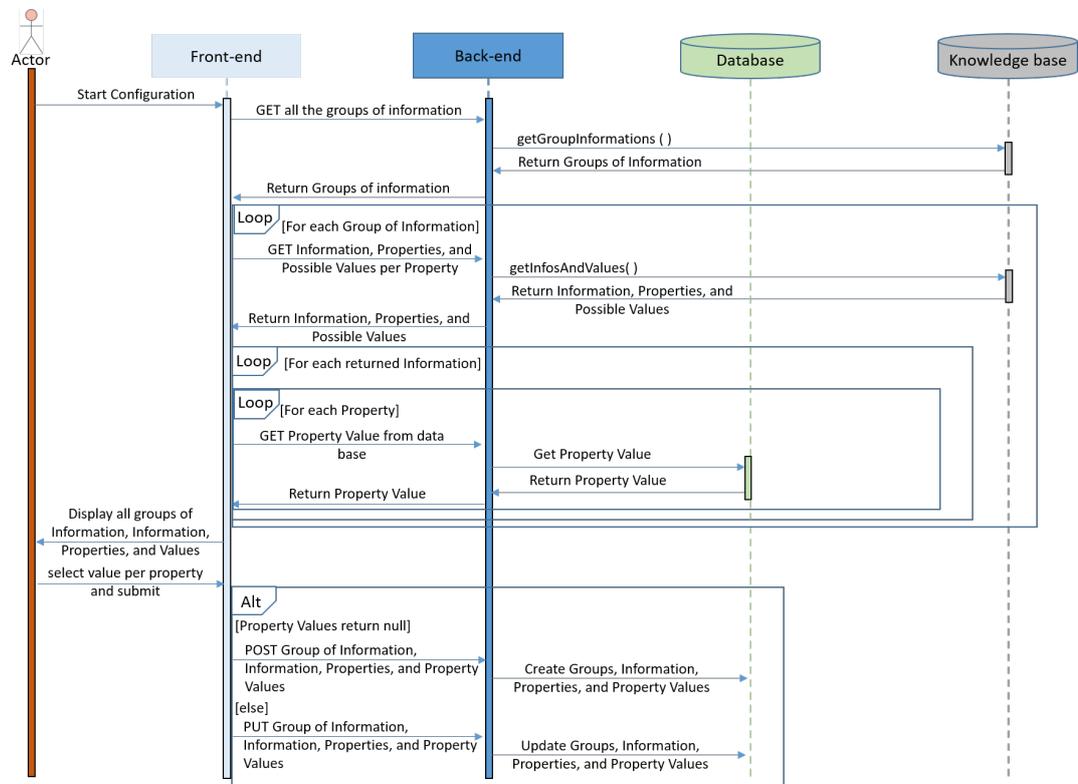


Figure 6.14: Sequence diagram for configuration of specifications.

information elements have the same name. Hence, it is essential to differentiate them by using the name of the group of information. Based on this request, a corresponding SPARQL query will be executed on the knowledge base ResOnt and different groups of information are returned to the front-end passing through the back-end. When those groups are returned, it is essential to retrieve the information that compose each group of information. Moreover, the information properties and possible values shall be retrieved. Hence, for each returned group of information, a GET request is transmitted from the front-end to the back-end in order to retrieve those information, properties, and possible values. Accordingly, corresponding SPARQL queries are executed on the knowledge base to extract the related information, the properties, and the possible values. Figure 6.15 shows a SPARQL query that retrieves different information of the groups entitled *Centres Cartography*. Moreover, it retrieves different information properties and possible values. As we can see in Figure 6.15, the group of information entitled *Centres Cartography* has different information. Those information have identical properties where every property has a set of possible values that are instances in

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

SPARQL query:

```

SELECT ?Information ?Property (group_concat(?PossibleValue) as ?PossibleValues)
WHERE {
  ?GroupOfInformation rescrc:HasInformation ?Information.
  VALUES ?GroupOfInformation{resrc:CentresCartography}
  ?Information rdf:type ?Domain.
  ?Relation rdfs:domain ?Domain.
  ?Relation rdfs:range ?Property.
  filter (?Domain not in (owl:NamedIndividual))
  (SELECT *
WHERE {
  ?PossibleValue rdf:type ?Property .
})
}

```

Information	Property	PossibleValues
Address	InformationCategory	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Spatial http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Spatial"
Address	degree of criticality	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Extreme http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Extreme"
Address	Data Type	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Integer http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Integer"
Address	InformationalComponent	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#ComboBox http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#ComboBox"
Address	Orientation	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Circular http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Circular"
Address	FieldType	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Obligatory http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Obligatory"
Distance	InformationCategory	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Spatial http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Spatial"
Distance	degree of criticality	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Extreme http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Extreme"
Distance	Data Type	"http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Integer http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#Integer"

Figure 6.15: SPARQL Query for retrieving different information, properties, and possible values for a group of information.

the ontology. Once retrieved, those information, properties, and possible values are returned to the front-end. Before displaying the different information, properties and possible values to the user, it is required to check which properties were already configured and stored in the database if any. The importance of this test is to avoid the repetition of the total configuration. Hence, for each information, the front-end will transmit a GET request in order to get the value of each property. Based on this request, the back-end will extract the property value from the database and return it to the front-end. Once done, the totality of the groups of information, information elements per group, properties per information, possible values, and configured values will be displayed to the user through the graphical interface. Hence, for each information contained in the groups of information, the user will select a value per property and submit her/his choices. When the user's choices are submitted, it is essential to store the selected values in the database for further retrieval. Hence, a POST request will be transmitted to the back-end in order to update the groups of information, information, properties, and property values in the database if they were already configured. Whereas, if those groups and information were not already configured, a PUT request will be transmitted from the front-end to the back-end for their creation in the database. Similarly to the context and task creation activities, in order to ensure the required functionalities in the specifications configuration, it is necessary to instantiate ResOnt ontology and relate those instances. In this context, we instantiated different information properties in ResOnt ontology. For instance, an informational component can be Text field, Radio button, Checkbox, List, Date and time

6.5 Dynamic and customised system and interface design

picker, and Combo box. Regarding the field type, it can be whether optional or mandatory. In addition to the ontology instantiation, in order to ensure the functionality of the system based on those specifications, it is essential to integrate different functions related to those specifications and execute those functions based on the selected values. We notice that, in this thesis, we only consider two specifications that are: Informational component, and Field Type. However, it is essential to take the totality of specifications into consideration. Moreover, it is strongly required to make the difference between input and output interface components. In this thesis, we only consider informational components that can be used for input and output at the same time. Those components are Text Field, Radio button, Check box, Date and Time picker, and combo box. Therefore, we are aware of the limitation of this work in this context. Figure 6.16 illustrates an example of the configuration of different properties for the group of information entitled Victims General Information.

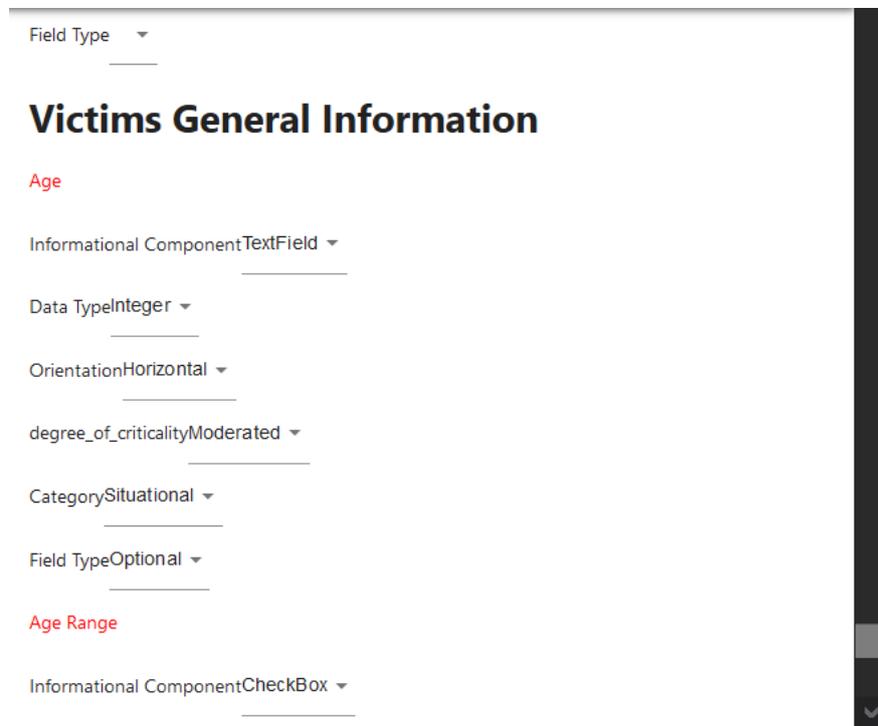


Figure 6.16: Configuration of specifications in MODES platform.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

6.5.2 Template creation

After having configured the system's specifications by its administrators and identified different contexts by the system's end-users, it is essential to design the graphical interfaces of the system by those end-users. There exist several approaches for designing user interfaces. Multiple solutions have been developed to validate these approaches. Although each approach has its context and domain of application, none of them is complete in a way that allows end users of a collaborative communication system to design the system's and interfaces in a personalised way. On the one hand, some of those previous approaches impose the implication of domain experts, designers, and developers to achieve the design and development phase, which may increase the cost and interaction problems. On the other hand, other approaches that allow final users designing and developing software objects and interfaces impose the construction of domain models by the end-users themselves. Accordingly, thanks to the template creation activity, the proposed solution helps overcoming those limitations by allowing end-users creating personalised templates based on pre-defined models inspired from operational practices. In this context, the proposed solution enables end-users creating personalised templates as well as integrating and positioning different different components on the graphical interface. Moreover, it allows the adaptation of a template's size according to the communication instrument's interface by adopting an approach based on responsive interfaces. In this activity, based on the property values of information elements, the elements of each group will be placed in the right informational component that will be positioned on the created template. We notice that, in order to enhance the use of the system by its end-users including the design of the interface, it is essential to define a set of possible values for several information elements. The reason behind this requirement is two-folded. First, for some informational components represented by checkboxes, radio buttons, and combo boxes, the set of possible values must be defined in order to obtain a functional communication system. Second, in order to ease the end-users' tasks during the use of the communication system, it is necessary to support those users by proposing to them the possible values of information elements to select. We also notice that not all the information elements can have a set of possible values. For example, the name of a victim cannot be predicted in advance. Accordingly, classes that represent those information elements must be instantiated based on the rescue domain knowledge in order to be retrieved in the design and the usage of the system. Examples of

6.5 Dynamic and customised system and interface design

those information are: Organization Member Role, Affiliation, Agent Function, Age Range, Availability, Function of Responsible, Incident, Material, Material Status, Role of Responsible, Sex, Site Function, Site Type, Skills, Skills of Responsible, Victim Status. Moreover, the end-users should have the ability to integrate the required media components in the created template. Those templates will be then retrieved in the communication system in order to transmit, receive, and visualise information. Figure 6.17 illustrates a sequence diagram for the template creation activity. As we can see in Figure 6.17, when the user starts the template creation, the user id will be retrieved automatically based on the authentication phase (Cf. Section 6.6.1). A request is then transmitted from the front-end to the back-end in order to get the possible contexts based on the user id. Therefore, those contexts will be retrieved from the database and returned to the end-user passing through the back and front-end. When different retrieved contexts are displayed to the user, this latter will select a specific context and submit her/his choice. When the user's choices are submitted, different groups

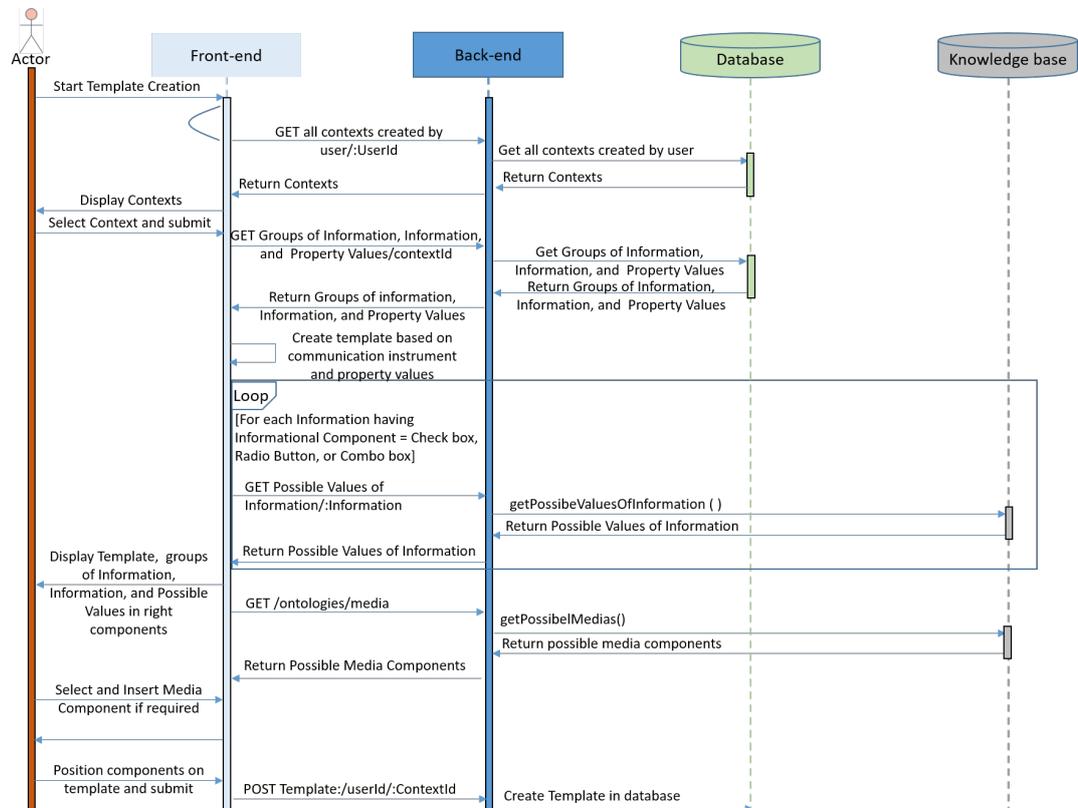


Figure 6.17: Sequence diagram for template creation.

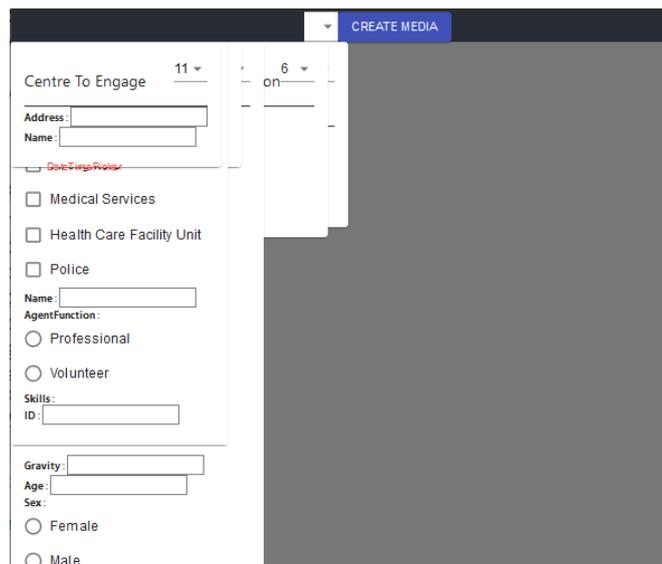
6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

of information, information elements, and property values should be retrieved based on the selected context. Hence, a new GET request is transmitted from the front-end to the back-end in order to retrieve different groups, information, and property values based on the context id. Accordingly, those parameters and values will be retrieved from the database and returned back to the front-end passing through the back-end. Based on the communication instrument used in context, and the different property values retrieved, a corresponding template will be created in the front-end. In this context, the size of the template will be adapted to the size of the communication instrument's interface by adopting an approach based on responsive interfaces. Moreover, different information will be placed in the right components on the basis of the informational component selected. In addition, for each information having a check box, radio button, or combo box as an informational component, it is necessary to retrieve the possible values of information from the knowledge base. Hence, a GET request is transmitted from the front-end to the back end containing the name of information. Accordingly, a corresponding SPARQL query will be executed on the knowledge base and different instances of the information are returned back to the front-end passing through the back-end. The front-end will then display different groups of information, information, and possible values of information in the right informational components on the created template. Afterwards, a new GET request will also be transmitted from the front to the back-end in order to retrieve different media components. Therefore, those components will be retrieved and returned to the user through the back-end and the front-end. On the basis of the returned media components, the end-user will be able, if required, to select the desired media component and insert it on the template. Hence, a corresponding interface component will be displayed on the template with other informational components displayed previously. After having inserted the required media components, the end-user will be able to position different groups of information and media components on the template. Two cases of positioning are possible to the user. The first case is applied for contexts that contain Desktop, Laptop, or Tablet as Communication instrument. In this case, the users will be able to change the positions of components in different ways and multiple components can be placed horizontally at the same line. To this end, drag and drop functions can be used. Whereas, the second case is applied for contexts that are based on the usage of Smartphone. In this case, the end-users should be able to change the order of different components while respecting the limitations of a smartphone interface. For instance, no more than two components can be placed together horizontally

6.5 Dynamic and customised system and interface design

at the same line in order to respect the borders' limitations. To this end, the grid functions of material design can be used. Those functions allow the adaptation of different components on the basis of the smartphone interface. Once the design of the template is finished, the user can submit her/his choices. When the user's choices are submitted, the front-end will transmit a POST request to the back-end containing the context id, the user id, and the template in order to create this latter in the database for further retrieval.

As it has been mentioned previously, in order to ensure some of the functionalities required for template creation, it is essential to instantiate the ontology for this aim. Accordingly, we have instantiated different information classes for which possible values should be retrieved. Moreover, it is essential to define different instances for media components. Hence, we instantiated the class Media component into different output components specifically Signal component (E.g. ECG), Map Component, Photo Component, and Video Component. However, in this thesis, we do not take input media components into consideration. We are aware of this limitation in our work. Figures 6.18 and 6.19 illustrate an example of template creation based on the context created in Figures 6.6 and 6.7. As we can see in Figure 6.18, on the basis of the created context and the configured specifications, different groups of information are located in separated blocks containing multiple information elements. The aim of this separation is to enable the end users to transmit and receive those groups independently. In addition, each information



The screenshot displays a web interface for creating a media template. At the top right, there is a blue button labeled 'CREATE MEDIA'. Below it, the form is organized into several sections:

- Centre To Engage:** A dropdown menu showing '11'.
- Address:** A text input field.
- Name:** A text input field.
- Get Press Photo:** A red button with a camera icon.
- Service Selection:** Three checkboxes for 'Medical Services', 'Health Care Facility Unit', and 'Police'.
- Name:** A text input field.
- AgentFunction:** Two radio buttons for 'Professional' and 'Volunteer'.
- Skills:** A text input field.
- ID:** A text input field.
- Gravity:** A text input field.
- Age:** A text input field.
- Sex:** Two radio buttons for 'Female' and 'Male'.

Figure 6.18: Creation of template in MODES Platform.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

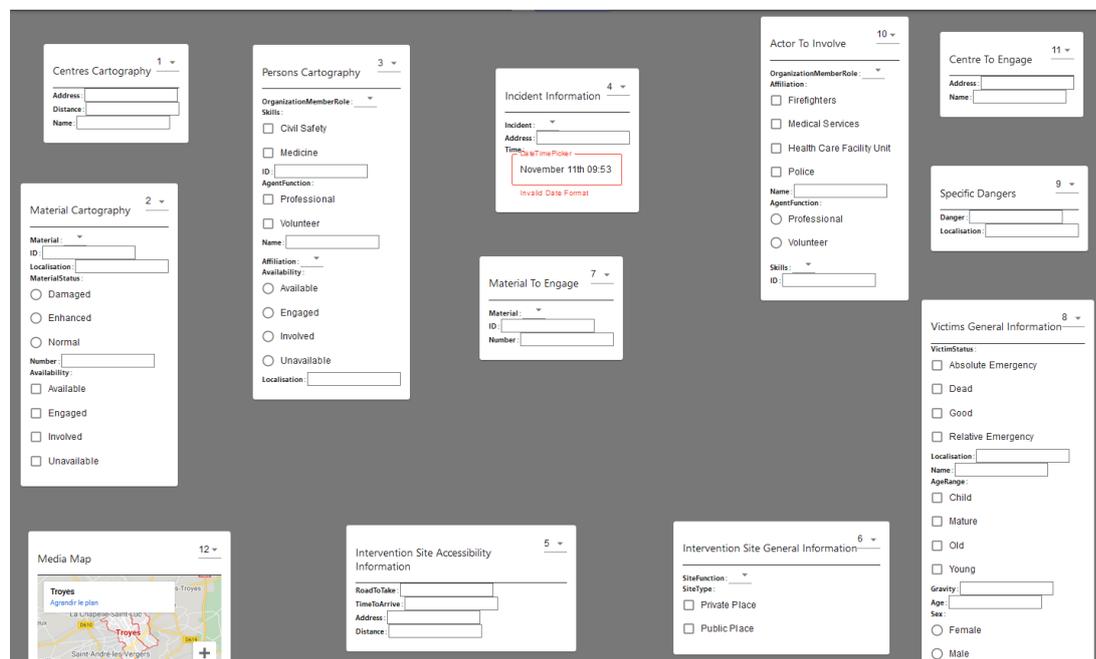


Figure 6.19: Positioning of components and integration of media components in MODES Platform.

is placed in the right informational component on the basis of the informational component selected in the configuration of specifications. Moreover, fields that are configured as obligatory are highlighted by using a red star symbol. Hence, the user will be able to integrate the required media component in the created template. For instance, in this example, we have selected the map component to be integrated. Afterwards, the user will position those groups in a way that meets her/his preferences in order to obtain a final personalised template as shown in Figure 6.19. We notice that there exist two ways for positioning different blocks: (1) Changing the positions manually using drag and drop; (2) Changing the order of the group on the interface. In the case of using desktop, laptop, or tablet, users are able to choose the way they prefer. However, in case of a Smartphone, the positioning method is limited to the second way. The obtained template will be then retrieved in the communication system.

After having identified different contexts and created different templates, the end-users should be able to use the obtained communication system to exchange and visualise information while respecting the access control policy. In the next section, we present different functionalities required to allow communication through

the designed system. In addition, we present the access control and rights management policy.

6.6 Communication and Access Control

As mentioned in section 6.2, the third principle of the proposed solution consists in ensuring efficient communications and confidential access to information. In this context, using the designed system, end-users must be able to exchange, receive, and visualise information based on the context of usage. Related to information confidentiality, multiple mechanisms must be integrated such as data encryption, authentication, access control, as well as other mechanisms related to the security of communication infrastructure. However, in this work, we only focus on a single mechanism that is access control in the communication system since other mechanisms like data encryption can be ensured with standard tools. We are also aware of the limitation of our work in this context. Figure 6.20 shows a use case diagram for MODES communication system. As we can see in Figure 6.20, the communication activity consists of four sub-activities that are: (1) User Authentication; (2) Connexion to intervention and context selection; (3) Information reception and consulting; and (4) Information transmission. User authentication is an activity required in different other activities as discussed previously. Achieved by the platform's end-users, it serves mainly for guaranteeing confidential access to the platform as well as extracting users' identities and roles. Regarding the connexion to intervention and selection of context, this

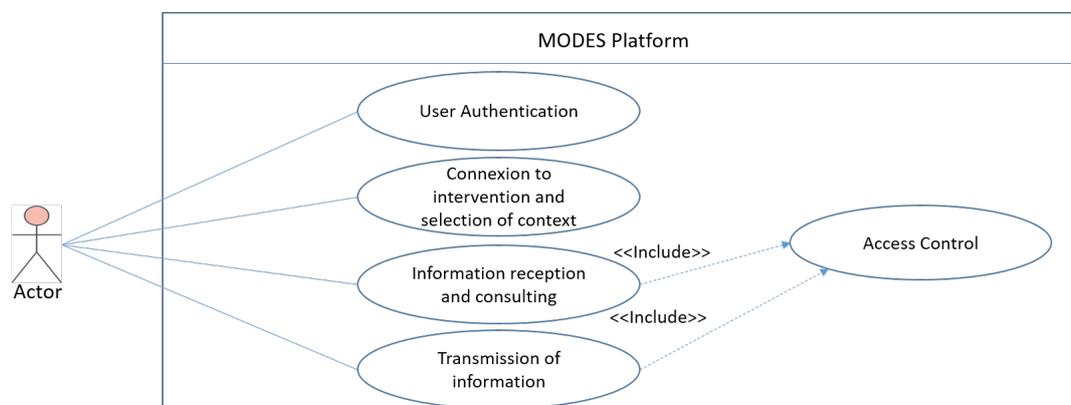


Figure 6.20: Use case diagram for MODES communication system.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

activity lies within selecting a target intervention through a set of created interventions, and specifying the user's context in the intervention in order to retrieve the appropriate template created previously. Hence, this activity should also be achieved by the system's end-users. After having being authenticated, connected to an intervention, and retrieved the appropriate interface, end-users should be able to communicate through the obtained system by (1) Information reception and consulting; and (2) Transmission of information. In order to simplify the user's tasks in communication, we propose to allow the user to transmit and receive required groups of information as presented in the interaction model instead of transmitting or receiving each information element apart. We notice that transmission of information includes several sub-tasks achieved before this transmission that are Creation and Update, or Deletion of information. Moreover, in order to ensure the confidential access to information, the last two activities must include access control activity guaranteed by the system itself.

6.6.1 User authentication

Since the platform is based on designing and implementing a personalised communication system that guarantees the confidentiality of information, it is essential to integrate an authentication mechanism. The motivation behind integrating an authentication process is two-folded: An authentication will guarantee a confidential access to the system and constitutes a required mechanism for access control. It also serves for determining user's roles and identity based on their credentials stored in the database. We notice that the authentication process is required before different activities in the platform that are: Context Creation, Task Creation, Specification Configuration, Template Creation, Connexion to intervention, and Communication. Several methods can be used for authenticating a system's users. In this context, we have adopted an authentication mechanism based on the JSON Web Token (JWT) [Jones *et al.*, 2015]. There are several benefits to using JWT authentication. A JWT is a secure method of exchanging information. Thanks to this mechanism, information is exchanged in the form of a signed token so that it can be verified for legitimacy. Moreover, JWT can use a public/private key pair in the form of an X.509 certificate for signing. A JWT can also be symmetrically signed by a shared secret using the HMAC algorithm for security reinforcement. Figure 6.21 illustrates a sequence diagram for the user authentication mechanism integrated into the platform based on JWT. As we can see in Figure 6.21, with each new connexion, the end-user is redirected

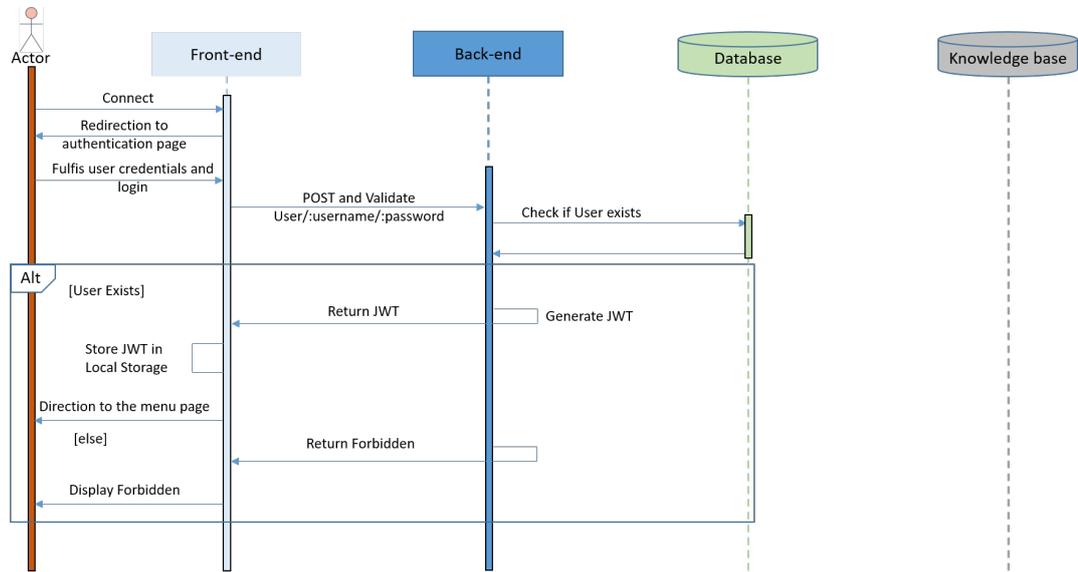


Figure 6.21: Sequence diagram for user authentication.

to the authentication page. Hence, s/he fulfils her/his credentials and submits. Once done, those credentials are transmitted from the front-end to the back end in order to validate the existence of the user in the database. Hence, the back end will query the database for this verification. If the user exists, an access token (JWT) will be generated at the back-end and transmitted back to the front-end for local storage. This token will be then transmitted with each HTTP request from the front to the back-end. In this case, the user will have access to the platform and directed to a menu page. However, if the user does not exist in the database, the back-end will return Forbidden to the front-end and the response will be displayed to the user.

In order to retrieve the user's role based on the authentication phase, it is essential to store her/his role in the database together with her/his credentials. We notice that a user's role corresponds to an instance of organisation member role defined in the knowledge base.

6.6.2 Connexion to intervention and context selection

After having being authenticated in the platform, created different contexts and templates, the end-user will proceed to use the communication system. In this context, one must select a specific intervention through a set of created interventions. Moreover, the context of usage must be selected through a list of contexts

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

created by the user previously. Figure 6.22 illustrates a sequence diagram for intervention and context selection. As illustrated in Figure 6.22, when the end-user connects to the communication system, the user id will be retrieved automatically based on the authentication phase (Cf. Section 6.6.1). At the same time, a GET request will be transmitted from the front to the back-end in order to retrieve all the created interventions. Therefore, those interventions will be retrieved from the database and returned to the end-user passing through the back and front-end. When different retrieved interventions are displayed to the user, this latter will select a specific intervention and submit her/his choice. When the user's choices are submitted, different contexts of usage created by the user should also be retrieved. Hence, a new GET request is transmitted from the front-end to the back-end in order to retrieve different contexts based on the context id. Accordingly, those contexts will be retrieved from the database and returned back to the end-user passing through the back and front-end. Hence, the end-user will select a context and submit. When the user's context is submitted, the appropriate template should be retrieved. Accordingly, a new GET request is transmitted from the front to the back-end in order to retrieve the template based on the user id and context id. Therefore, the corresponding template will be retrieved from the database and returned to the end-user passing through the back and front-end. Following the intervention and context selection activities, the end-

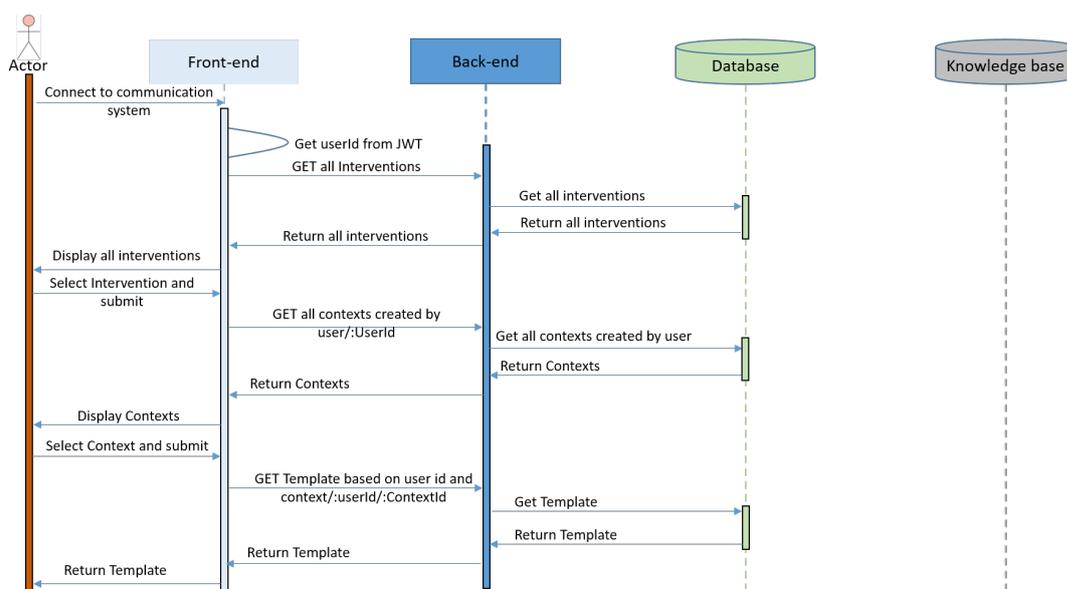


Figure 6.22: Sequence diagram for intervention and context selection.

user will proceed to the communication activity. As mentioned previously, in order to ensure confidential access to information, the communication activity must include access control and rights management. To this end, we have defined an access control and rights management policy that aims at controlling different user's actions in this context. More details about this policy are provided in [6.6.3](#).

6.6.3 Access Control and Rights Management

Before presenting the access control and rights management policy, let us discuss the intent of this policy as well as different requirements in terms of access control. In this thesis, we propose an information exchange system oriented for rescue operations. This system will be used by different rescue actors involved in rescue interventions. A large number of rescue interventions are managed by multiple organisations. Each intervention requires the involvement of one or several teams where each team is composed of multiple organisation members. Moreover, every organisation member has a specific organisational member role, is affiliated with an organisation, and execute different tasks based on her/his role. During an intervention, a large number of private information is exchanged such as personal and medical information. Hence, the first requirement of controlling access in the system is to forbid any external access to those information. Moreover, based on their roles and tasks, participating actors should have different access rights on information. Hence, it is essential to define different access rights on information. Permissions must then be controlled based on those rights and the executed actions. Those permissions must not only depend on the access rights defined. Indeed, permissions and restrictions should also depend on other assignments such as users to team and teams to intervention assignment. For instance, users that do not participate in a certain intervention should not have the permissions for accessing information exchanged in this intervention. Several access control models have been proposed in the literature. Those models were proposed on the basis of distinct requirements and purposes. Indeed, designing or adopting an access control model depends strongly on several dimensions such as the intent of this control, the required level of security, and the domain of application. Access control models started with classic models and have evolved lately to more complex ones. In this context, two classic models were proposed: the Discretionary Access Control (DAC) and the Mandatory Access Control (MAC). The

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

two aforementioned models were employed to facilitate the management of access control in different systems. The DAC model, also called the Identity Based Access Control (IBAC) model, consists of restricting the access right to each and every resource based on the user's identity [Downs *et al.*, 1985]. A main limitation of DAC is that systems' administrators might have difficulties in giving access permission to the users in case of large systems and environments. On the other hand, MAC ensures security access control by means of security labels. In this context, it attaches security labels to each user and resource [Bell & La Padula, 1976]. The resource labels are classified from unmarked to top secret. The access right is then given to the users based on their labels and the resources labels. Unfortunately, similarly to DAC models, MAC implies defining permissions based on user identities and labels. In addition, this model is costly to implement. In order to overcome the limitations of classic access control models, an alternative model was proposed and entitled: Role-Based Access Control (RBAC) model [Sandhu *et al.*, 1996]. RBAC model takes into consideration the user's role and thus different permissions are assigned to those roles. The main limitation of this model is that roles' permissions are set on object types but cannot be specified to an individual object instance. Hence, this is inadequate in collaborative environments because users might require particular authorisation for particular objects. Moreover, in this model, it is not possible to define permissions based on teams' compositions and activities. Another alternative solution proposed by Thomas [1997] is called Team based Access Control (TMAC). This model defines two essential aspects of the context of collaboration: Object context, and User Context. User context serves for identifying particular participants who play a role in a team at any given time. Regarding the object context, it defines specific information or objects needed for collaboration purposes. Permissions in this model are associated and assigned to roles and teams. Unfortunately, TMAC lacks the collaborative concepts characteristics such as tasks associated with each role. Other access control models were developed to coordinate the permissions with respect to the tasks in progress and the workflow instances. In this context, the Task Based Access Control (TBAC) model [Thomas & Sandhu, 1993] was designed to control different permissions based on users' tasks. In the TBAC model, permissions are assigned to tasks and users get permission while the task is in execution. Although this model may be sufficient for some use cases, this model is limited in our context since it does not consider the role assigned to each user. To this end, in collaborative environments, TBAC must be used with other models. To overcome those limitations, the Task-Role Based Access Control (T-RBAC) was

proposed [Oh & Park, 2003]. T-RBAC puts the tasks between the permissions and the roles. In other words, permissions are identified based on Users-Roles assignments and as well as Tasks-Roles assignments. This model, however, does not consider the team or collaborative concept. In order to overcome those limitations, Zhou & Meinel [2007] proposed an alternative model called Team and Task Based RBAC (TT-RBAC) model. The TT-RBAC model takes into account five entities: user, role, permission, task, and team. In this context, users are assigned to roles and teams, roles and tasks are assigned to teams, and permissions are assigned to roles and tasks. The TT-RBAC can be so beneficial to control permissions in collaborative environments since it considers different parameters to take into account. In TT-RBAC, based on team membership, users have access to the resources of the team, which are identified on the basis of delegated tasks. However, for each user, the exact right s/he obtains from a team is determined by her/his role and the team's activity being executed [Zhou, 2008]. Figure 6.23 illustrates the Core TT-RBAC model. It shows different parameters and relations defined in this model. We notice that relations between different elements are many-to-many. As we can see in Figure 6.23, TT-RBAC model consists of a set of sessions where each session is a mapping of one user to many possible

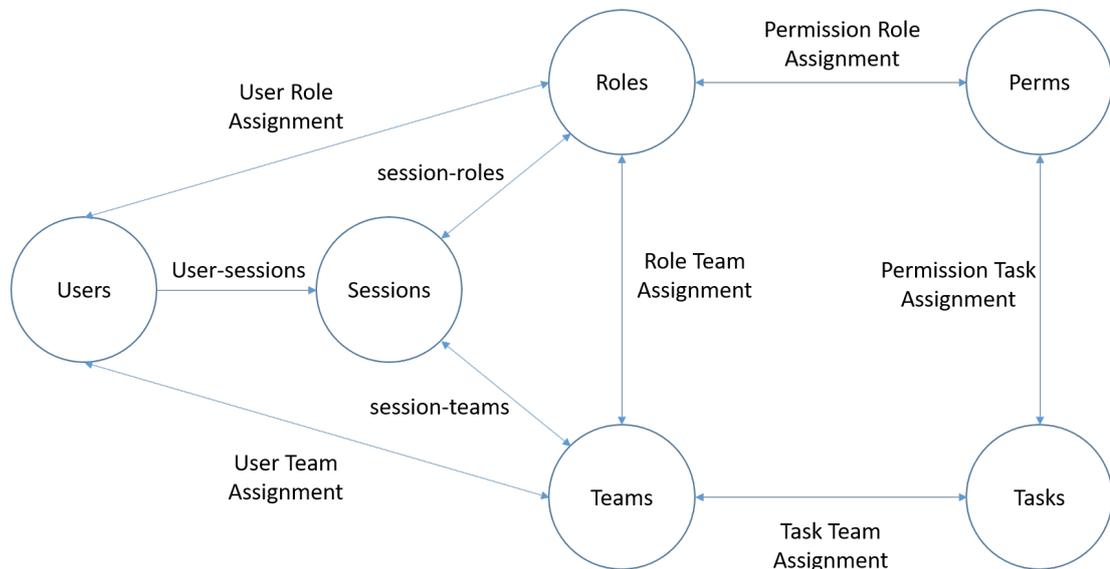


Figure 6.23: Illustration of Core components from TT-RBAC and interaction between them.

*Source [Zhou & Meinel, 2007].

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

roles and teams. Each session is associated with a single user and each user is associated with one or more sessions. Three relations are defined in this context: User-sessions, session-roles, and session-teams. User-session is the mapping of a user onto a set of sessions. Session-roles is the mapping of a session onto a set of roles, whereas, session-teams is the mapping of a session onto a set of teams. Every team includes a set of users having different roles. In addition, each team has a set of different roles that can be activated by team members. Two relations are defined in this context: User-Team Assignment, and User-Role Assignment. Besides, different teams have different assigned tasks that can be activated by the team's members. Through different roles and tasks, permissions are assigned to teams. In other words, in TT-RBAC, roles and tasks are associated with a set of permissions that are then assigned to teams. Although its benefits in collaborative environments, TT-RBAC cannot be adopted completely in our solution due to many reasons. Hence, we will modify this model and adapt it to fit better the operational needs. First, tasks in the TT-RBAC are assigned to different teams. However, in rescue operations, tasks are assigned to the roles of users and roles are then associated with different persons. For example, a rescuer and a driver do not share identical tasks even in the same team. Second, TT-RBAC considers the notion of sessions where each session is associated with a single user that can be associated with different roles and teams in a session. In rescue interventions, users should be associated with teams that are associated with interventions. Third, different roles associated with a user are activated by the team members themselves. During rescue interventions, this might cause serious problems since team members do not have the time to activate each role in a context. In a rescue intervention, a user has a specific organisation role that is usually assigned by a responsible. Fourth, in the TT-RBAC model, tasks' instances are always related to states such as active and inactive and permissions depend on this state. In the context of rescue interventions, it is difficult to determine the tasks' states which may cause problems in permissions. Eventually, permissions in the TT-RBAC are defined based on tasks and roles while different access rights are not considered. However, while access control aims at controlling permission on different information, access rights on those information must be considered. Accordingly, we have replaced the session in TT-RBAC with Intervention. In addition, we have assigned tasks to roles, which are assigned to users. Moreover, we have included the element *Access right* where access rights are assigned to tasks and roles respectively. Eventually, we assigned permissions to teams and access rights.

6.6 Communication and Access Control

Permission in this context includes a set of operations that refer to the user's actions, and objects on which those actions are executed. Figure 6.24 illustrates the obtained access control model based on the adaptation of TT-RBAC. We notice that, similarly to TT-RBAC, different relations are many-to-many except the user role assignment. Indeed, during a single intervention, a user should have a unique role that is defined previously. Different elements of the proposed model for access control are summarised as follows:

- **Users:** Different organisation members that will use the communication system. They represent a team's members that participate in an Intervention.
- **Role:** Organisation member role that can be assigned to different Users.
- **Teams:** Different Teams that takes part in an Intervention and include several Users with different Roles. We notice that one or more teams can be associated with an intervention.
- **Tasks:** Different Tasks that are associated with a Role depending on operational practices.
- **Intervention:** Mapping onto a set of Teams.

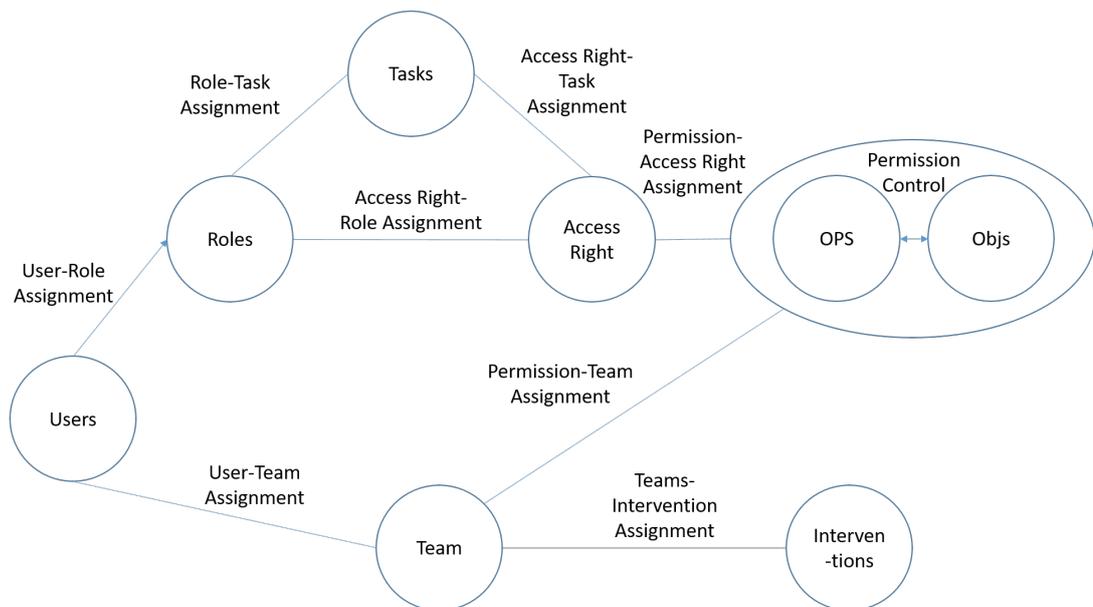


Figure 6.24: Access control model based on adapted TT-RBAC.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

- **Access Right:** The rights that a Role has on an Object type that are assigned to Roles and Tasks. Object type represents a group of information in our case.
- **Permissions:** Approval to perform an Operation on one or more Objects that have an Object Type. In other words, it consists in authorising or forbidding an action on information that belongs to a specific group of information.
- **Operation:** An action that a user executes on an Object.
- **Object:** An information on which an Action (read, create, delete, update) is executed.

As we can see in Figure 6.24, different elements of the model are related on the basis of distinct assignments. Some of those assignments are static and represented through knowledge in ResOnt. Those are:

- **Role-Task Assignment:** The assignment of role to a task. It lies within identifying different tasks that are associated with an organisation member role.
- **Access Right-Task Assignment:** The assignment of access rights to tasks. This relation consists in identifying the access rights on an Object type required by this task.
- **Access Right-Role Assignment:** The assignment of access rights to roles. This relation serves for determining the access right that an organisation member role has on an Object Type. Access Right-Role Assignment is determined on the basis of Role-Task Assignment and Access Right-Task Assignment.
- **Permission-Access Right Assignment:** The assignment of permissions to different access rights. It serves for controlling access on the basis of access rights.

On the other hand, other assignments are dynamic and can be employed through relating dynamic data in the database. Defining those assignments is of responsibility of the system's administrator. Those assignments are:

- **User-Role Assignment:** The assignment of a user to a role. This relation

corresponds to the assignment of an organisation member to an organisation member role.

- **User-Team Assignment:** The assignment of a user to a team. It represents the mapping of a user onto a team.
- **Teams-Intervention Assignment:** The assignment of teams onto an intervention. This relation consists in identifying the teams that participate in an intervention.
- **Permission-Team Assignment:** The assignment of permissions to different teams. In a given intervention, those permissions are assigned to the teams that take part of the intervention. They are then assigned to users based on User-Team Assignment.

After having modelled all the elements of the system and their relations, it is necessary to propose the mechanism for controlling access on the basis of the proposed model. Based on the proposed Access control model illustrated in Figure 6.24, it is essential to define different access rights. On the basis of those rights and different assignments, permissions for different actions can then be controlled. Figure 6.25 shows a use case diagram for access control and rights management. As we can see in Figure 6.25, the access control and rights management activity consists of two sub-activities: Rights management, and Permissions control. The rights management activity precedes the permissions control. It mainly serves for determining the access rights. This is achieved through the association Access Right-Role Assignment. This activity is generally achieved by a system's adminis-

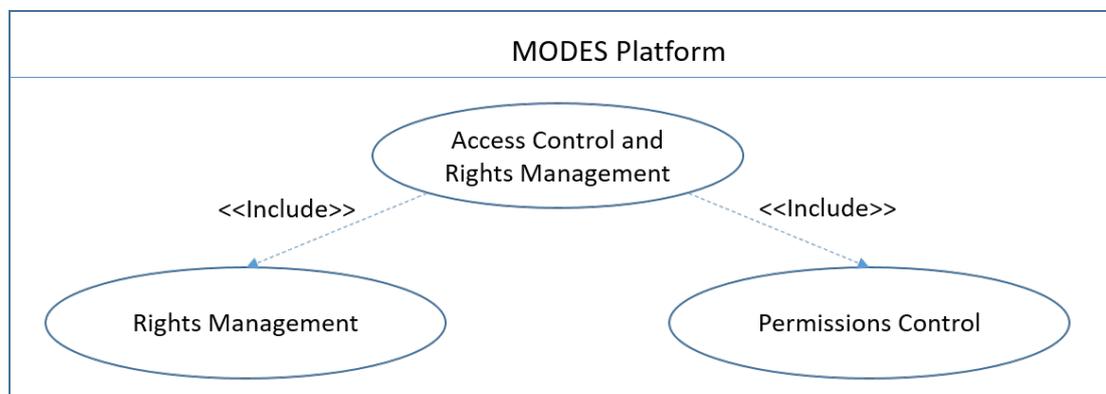


Figure 6.25: Use case diagram for Access Control and Rights Management.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

trators before the usage of the system. Whereas, the permissions control activity consists in controlling different actions on information during the run time of the system based on those rights, the assignments between different parameters, and the access control policy.

6.6.3.1 Rights management

Generally speaking, four relations can exist between an organisation member role and a group of information in terms of access rights as follows: *Has Read Access On*, *Has Write Access On*, *Has Write And Read Access On*, and *Has No Access On*. Each one of those relations will serve for determining the allowed actions that can be executed on an information value of a group of information. For instance, if a certain role is related to a group through the relation *Has Write Access on*, this means that each organisation member that has this role cannot execute read actions on the information values of the group. We notice that access rights are determined based on groups of information and not information elements since different information elements that belong to different groups of information may have the same names. Two types of assignment are required to determine the Access Right-Role Assignments as follows: Access Right-Task Assignment, and Role-Task Assignment. In other words, in order to identify the access rights that a role has on a certain group of information, different tasks assigned to the role must be considered. Moreover, different access rights assigned to those tasks must be taken into consideration. In Chapter 5, we mentioned that each task is associated to an organisation member role and produces or uses one or several groups of information. In addition, every task is attached to a computational functionality that can be Reception and Consulting, or Fulfilment and Transmission. Accordingly, we propose to determine different access rights based on those assignments and relations. The importance of using the relation between a task and functionality is to determine the access rights based on those functionalities instead of identifying them based on each task apart. Moreover, we propose to determine those rights automatically using SWRL rules [Horrocks *et al.*, 2004] instead of defining them manually. SWRL rules are in the form of inference between an antecedent and consequent. The intended interpretation can be expressed as follows: whenever the conditions stated in the antecedent hold are held, the conditions specified in the consequent must also be held [Horrocks *et al.*, 2004]. We notice that SWRL allows the insertion of relations between ontology instances based on other relations. To this end, we have instantiated the concept

6.6 Communication and Access Control

Functionality defined in the Design module into Reception and Consulting, and Fulfilment and Transmission. Reception and Consulting is used to determine the relation *Has Read Access On* between a role and a group of information. Indeed, if a certain task is attached to reception of consulting, the role to which this task is associated to should have read access on the group of information produced or used by this task. Whereas the second one serves for determining the relation *Has Write Access On* between a role and a group of information. In addition, we have related each instance of task to a functionality through the relation *Is Attached To*. For example, the task entitled *Fulfilment of call information in the system* is attached to *Fulfilment and Transmission*. We notice that several other instances and relations are required in this context such as the relation between a task and a group of information. Those instances and relations were discussed previously in sections 6.4 and 6.5. Table 6.1 shows different SWRL rules required for determining Access Right-Role Assignment based on Access Right-Task Assignment, and Role-Task Assignment. Thanks to those rules, it is possible to identify the access right that an organisation member role (r) has on a group of information (g) on the basis of tasks (t) associated to the role, groups of information produced or used by each task, and the functionality that each task is attached to. We notice that the prefixes *resd*, *resac*, and *resrc*, in Table 6.1, represent the Design, Access control, and Rescue and Communication modules in ResOnt respectively. As we can see in Table 6.1, each rule includes design properties, communication properties, and access control properties. The first two rules, R1 and R2, automatically set the different organisation member roles that have *Read Access* on a group of information. Indeed, if a task is associated to an organisation member role, is attached to reception and consulting, and produces or uses one or several groups of information, then this role must have a *Read access* on those groups of information. Regarding Rules R3 and R4, they serve for determining what are the different organisation member roles that have *Write Access* on a group of information. In this context, if a task is associated to an organisation member role, is attached to transmission and fulfilment, and produces or uses one or several groups of information, then this role should have a *Write access* on those groups of information. Based on the access rights obtained through those four rules, some organisation member roles could have write access and read access on certain groups of information. Hence, it is required to define the relation *Has Write And Read Access On* that relates the role to the group of information in this case as shown in R5 in Table 6.1. After having executed the SWRL rules presented in Table 6.1, it is required to delete the access rights that

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

Table 6.1: SWRL Rules for determining the relation between an organisation member role and a group of information in terms of access rights.

Ri	SWRL Rule
R1	resrc: OrganizationMemberRole(?r) \wedge resrc: Task(?t) \wedge resrc: GroupOfInformation(?g) \wedge resrc: Uses(?t, ?g) \wedge resrc: IsAssociatedTo(?t, ?r) \wedge resd: IsAttachedTo(?t, resd: ReceptionAndConsulting) \rightarrow resac: HasReadAccessOn(?r, ?g)
R2	resrc: OrganizationMemberRole(?r) \wedge resrc: Task(?t) \wedge resrc: GroupOfInformation(?g) \wedge resrc: Produces(?t, ?g) \wedge resrc: IsAssociatedTo(?t, ?r) \wedge resd: IsAttachedTo(?t, resd: ReceptionAndConsulting) \rightarrow resac: HasReadAccessOn(?r, ?g)
R3	resrc: OrganizationMemberRole(?r) \wedge resrc: Task(?t) \wedge resrc: GroupOfInformation(?g) \wedge resrc: Uses(?t, ?g) \wedge resrc: IsAssociatedTo(?t, ?r) \wedge resd: IsAttachedTo(?t, resd: FulfilmentAndTransmission) \rightarrow resac: HasWriteAccessOn(?r, ?g)
R4	resrc: OrganizationMemberRole(?r) \wedge resrc: Task(?t) \wedge resrc: GroupOfInformation(?g) \wedge resrc: Produces(?t, ?g) \wedge resrc: IsAssociatedTo(?t, ?r) \wedge resd: IsAttachedTo(?t, resd: FulfilmentAndTransmission) \rightarrow resac: HasWriteAccessOn(?r, ?g)
R5	resrc: OrganizationMemberRole(?r) \wedge resrc: GroupOfInformation(?g) \wedge resac: HasReadAccessOn(?r, ?g) \wedge resac: HasWriteAccessOn(?r, ?g) \rightarrow resac: HasWriteAndReadAccessOn(?r, ?g)

may cause a conflict. For instance, if the relations *Has Write And Read Access On*, *Has Write Access On*, and *Has Read Access On* exist between a role and a group of information, this will surely cause a conflict of access rights. In this case, it is essential to delete the relations *Has Write Access On* and *Has Read Access On* between the role and the group of information in case of existence of the relation *Has Write And Read Access On*. This deletion could be done manually or using a DELETE SPARQL query as shown in Figure 6.26. Moreover, in order to determine which groups of information are not accessible by a certain organisation member role, it is required to include the relation *Has No Access On* between the role and those groups. This relation should be inserted when

none of the access rights determined using the SWRL rules exists between the role and a group of information. The importance of this relation is to cover different relations that may exist between a role and a group of information in order to guarantee complete permissions control. Similarly to the deletion case, the insertion of the relation *Has No Access On* could be done manually or using an INSERT SPARQL query as shown in Figure 6.27.

6.6.3.2 Permissions control

After having identified different access rights, it is essential to define a policy for controlling users' actions mostly based on those rights, but not only. More formally, we refer to the permissions control that serves for determining whether a user's action on certain information is forbidden or authorized. We notice that different permissions must be controlled at the back-end. Hence, with each user's action, a request will be transmitted from the front to the back-end that will control permissions on the basis of several parameters and assignments and return the appropriate response to the front-end.

```

8 PREFIX resd: <http://www.semanticweb.org/SamerChehade/ontologies/2019/ResOntDesignOntology#>
9 PREFIX fn: <http://www.w3.org/2005/xpath-functions#>
10 PREFIX apf: <http://jena.apache.org/ARQ/property#>
11 DELETE
12 {
13   ?OrganizationMemberRole resac:HasReadAccessOn ?GroupOfInformation.
14   ?OrganizationMemberRole resac:HasWriteAccessOn ?GroupOfInformation
15 }
16 WHERE {
17   ?GroupOfInformation rdf:type resrc:GroupOfInformation.
18   ?OrganizationMemberRole rdf:type resrc:OrganizationMemberRole.
19   FILTER(Exists{?OrganizationMemberRole resac:HasWriteAndReadAccessOn ?GroupOfInformation}).
20 }

```

Figure 6.26: SPARQL Query for deleting existing access rights.

```

9 PREFIX fn: <http://www.w3.org/2005/xpath-functions#>
10 PREFIX apf: <http://jena.apache.org/ARQ/property#>
11 INSERT
12 {
13   ?OrganizationMemberRole resac:HasNoAccessOn ?GroupOfInformation
14 }
15 WHERE {
16   ?GroupOfInformation rdf:type resrc:GroupOfInformation.
17   ?OrganizationMemberRole rdf:type resrc:OrganizationMemberRole.
18   Filter((Not Exists{?OrganizationMemberRole resac:HasReadAccessOn ?GroupOfInformation}) && (Not
19     Exists{?OrganizationMemberRole resac:HasWriteAccessOn ?GroupOfInformation}) && (Not Exists{?OrganizationMemberRole
20     resac:HasWriteAndReadAccessOn ?GroupOfInformation}))

```

Figure 6.27: SPARQL Query for inserting the relation *Has No Access On* between a role and a group of information.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

Related to the communication between different end-users, we proposed to adopt a client-server approach. The client-side consists of different user's navigators whereas the server-side is composed of the back-end part and the database. In this context, mechanisms of data management will be centralised at the server-side. In addition, different information flow between clients will pass through the database as an intermediate point. Hence, the database will not only serve for archiving information for a long term period. But, it will serve also for storing and retrieving real time-data during the communication between different clients. For instance, when a user transmits information to another user, this information will be first stored in the database. It will be then retrieved by the second client from the database to be consulted by the second user. Similarly, when a user deletes information previously transmitted, that information will be deleted from the database and thus deleted at the second client interface. The main reason that motivated us to adopt this approach is that, thanks to this centralisation and the use of the database, it is possible to guarantee the traceability of different actions. In addition, this approach serves for storing different exchanged information for further retrieval in case of need.

Using the adapted TT-RBAC model that we have proposed for our purpose, several aspects must be considered in permissions control that are Access-Rights Permissions assignment, as well as different assignments between several other parameters such as Teams-Intervention assignment, User-Team assignment, Permission-Team assignment, and User-Role Assignment. Some of those Assignments are static such as the Access-Rights Permissions Assignment. Whereas other assignments are dynamic and change continuously like Teams-Intervention assignment, User-Team assignment, Permission-Team assignment, and User-Role assignment. Hence, we propose to control those permissions based on: (1) Static knowledge represented in the knowledge base; (2) Dynamic information stored in the database that includes Teams-Intervention Assignments, User-Team Assignments, and User-Role Assignments. Let us start with the first part of permissions control. This part consists in determining the access type based on static knowledge. Two types of assignments are required for this part of control: Access-Right Role Assignment and Permission-Access Right Assignment (See Figure 6.24). As it has been shown in 6.6.3.1, Access Right-Role Assignments are determined based on tasks associated to role, groups of information produced or used by a task, and the functionality attached to each task. Regarding the Permission-Access Right Assignment, we propose to define an access type for each combination of

action and access right. This access type can be whether forbidden or authorized. Based on this value of access type and the different dynamic assignments, permissions are controlled and a response is returned to the user according to her/his action. When using a database, four types of users' actions can be distinguished. Those actions follow the CRUD model that stands for Create, Read, Update, and Delete. In this context, for example, if the action is *Read* and the Access Right is *Has Read Access On* then the access type is *Authorized*. The response to the action in this case is *Authorized*. Whereas, if the action is of Write category such as Delete or Create, and the Access Right is *Has Read Access On* then the access type is *Forbidden*. Determining the access type based on knowledge represented in the ontology can be applied using a simple SPARQL query executed from the back-end on the knowledge base that will return the access type based on the user's action and access right. In order to determine the access type through the SPARQL query, different action's and access type instances must be included in the knowledge base. Accordingly, we have instantiated the concept *Action* into four actions: Read, Write, Update, and Delete. In addition, we have instantiated the *Access type* into Forbidden and Authorized. Following this instantiation, in order to define Permission-Access Right Assignments, it is essential to define which access type's instance is returned based on action-access right combination. Therefore, we have assigned a corresponding access type on the basis of each action-access right combination as shown in the algorithm 1. The function presented in Algorithm 1 represents the SPARQL query that will be executed by the back-end on the knowledge base in order to determine the access type. This function, called *GetAccessType*, has three inputs: the Action executed, the Group of information containing the information value on which the action is executed, and the Organisation member role of the person executing the action. Whereas the output of this function is an instance of Access Type in ResOnt. When this function is executed, the access right that relates the role to the group of information is first extracted. The access type is then returned based on combinations of input action and the access right extracted. For instance, if the access right is *Has No Access On*, the returned access type is then Forbidden whatever the action is. On the other hand, if the input action is Write, Create or Delete, and the access right is *Has Write Access On*, the returned access type is then Authorized. As being said, permissions control based on static assignments is complemented by the control of other dynamic assignments. Hence, at the back-end, other assignments related to dynamic information will be controlled and the final response of this control will be returned to the front-end and then

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

Algorithm 1: Selecting Access Type based on Permission-Access Right Assignment

Function *GetAccessType* (**Action, Group of Information, Role**) = (**AccessType**)

Input: Group of Information: Instance of Group of Information in ResOnt

Role: Instance of Organization Member Role in ResOnt

Action: Instance of Action in ResOnt

Output: Access Type: Instance of Access Type in ResOnt (Forbidden or Authorized)

```

1 Initialization;
2 Retrieve Access Right(Group of Information, Organization Member Role);
3 if Access Right = HasNoAccessOn then
4   | AccessType  $\leftarrow$  Forbidden;
5 else if Action = Create||Update||Delete && Access Right = HasWriteAccessOn then
6   | AccessType  $\leftarrow$  Authorized;
7 else if Action = Read && Access Right = HasWriteAccessOn then
8   | AccessType  $\leftarrow$  Forbidden;
9 else if Action = Create||Update||Delete||Read &&
   | Access Right = HasWriteAndReadAccessOn then
10  | AccessType  $\leftarrow$  Authorized;
11 else if Action = Create||Update||Delete && Access Right = HasReadAccessOn then
12  | AccessType  $\leftarrow$  Forbidden;
13 else if Action = Read && Access Right = HasReadAccessOn then
14  | AccessType  $\leftarrow$  Authorized;
15 Return AccessType;

```

to the user with each action of this latter. Figure 6.28 illustrates a sequence diagram that represents the procedure of permissions control in MODES platform. In order to check permissions as presented in Figure 6.28, it is necessary to define a permissions control policy on the basis of different assignments and actions. In this context, some tests are in common whatever the user's action is. However, other tests and policy requirements differ from action to another. Accordingly, in addition to the first algorithm presented previously, we propose three algorithms that serve for ensuring complete control of permissions based on users' actions. The first algorithm includes the policy for the action *Read*, the second one controls permissions in case of *Delete*, whereas the third one serves for authorising or forbidding actions *Create* and *Update*. Those algorithms refer to different functions implemented at the back-end. Inputs of those different algorithms come from the front-end and on the way back, the outputs are returned to the front-end.

6.6 Communication and Access Control

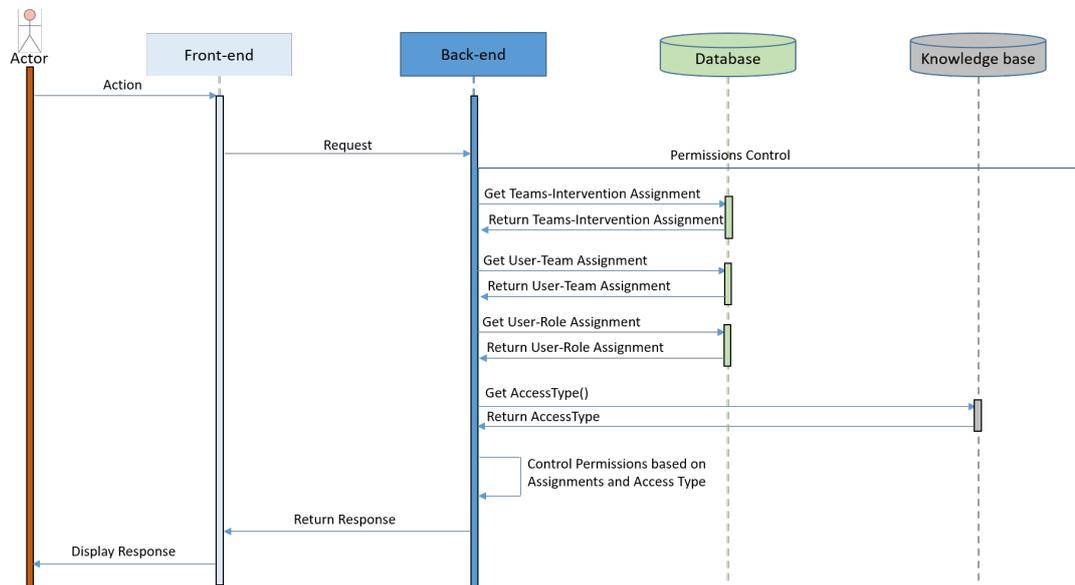


Figure 6.28: Sequence diagram for permissions control in MODES platform.

The first algorithm, called Read information value, serves for determining whether the user's request to read an information value is forbidden or authorized. In order to read an information value, a user should be authenticated, participates in the intervention in which the action is executed, and has the appropriate access right for reading the information. We notice that, if the user is the creator of a certain information value, s/he must be allowed to read this value even if s/he does not the required access right for this aim. Algorithm 2 represents the algorithm for reading information value. This algorithm is executed with each activity of information reception and consulting (Cf. Section 6.6.4). If this request is authorised, the information value will be retrieved from the database and returned to the user. Else, a Forbidden response will be returned to the user. Inputs of this algorithm are the name of the group of information containing the information value, the information name for which the value is requested, the user token, and the id of target intervention based on the user's selection. Whereas the output is the read response. This output might include the information value if the request is authorised. As we can see in this Algorithm 2, when a user requests reading an information value, a test of the user's authentication will be executed based on the access token submitted with the request. If the user is not authenticated, the Read response will be set as Forbidden and the user will be redirected to the authentication page. Else, a new test will be executed to continue the control

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

mechanism. The second test lies within determining if the user that executes the action takes part of the target intervention or not. In this context, the user's team is extracted from the database. In addition, different teams that participate in the intervention are retrieved from the database. If the user's team does not belong to different intervention teams, then the user does not participate in the

Algorithm 2: Read information value

Input: Group of Information: Name of group of information, Information: String that represents the information name, User Token: Access Token containing the user id, Id of Target Intervention

Output: Read Response: String, Information value

```
1 Initialization;
2 if User !Authenticated then
3   | Read Response  $\leftarrow$  Forbidden;
4   | Redirection to Authentication page;
5 else
6   | Check if user's team participates in Target Intervention;
7   | if User's team  $\notin$  Intervention teams then
8     | | Read Response  $\leftarrow$  Forbidden;
9     | | Return Read Response;
10  | else
11  | | Action  $\leftarrow$  Read;
12  | | Retrieve Role from database(User Token);
13  | | AccessType  $\leftarrow$  GetAccessType(Action, Group of Information, Role);
14  | | if AccessType = Authorized then
15  | | | Retrieve Information value;
16  | | | Return Information value;
17  | | else
18  | | | Check if user is creator(User Token, Information Value);
19  | | | if User = Creator then
20  | | | | Retrieve Information value;
21  | | | | Return Information value;
22  | | | else
23  | | | | Read Response  $\leftarrow$  Forbidden;
24  | | | | Return Read Response;
25  | | | end
26  | | end
27  | end
28 end
```

target intervention. Therefore, s/he should not be able to execute actions in this intervention. Hence, the Read Response will be set as Forbidden and returned to the front-end. However, if the user's team belongs to different intervention teams, a new test will be executed. This test aims at determining the access type based on the access right that the user's role has on the group of information. To this end, the organisation member role will be retrieved from the database using the user token. Moreover, the *Action* will be set as read and a SPARQL query that corresponds to algorithm 1 will be executed on the knowledge base to retrieve the access type. This query will take the action, the group of information, and the organisation member role as inputs. On the basis of the returned access type, if this latter is Authorized, the information value will be retrieved from the database and returned to the front-end to be displayed to the end-user. However, if the access type is Forbidden, the last test will be executed. This test serves for determining if the user is the creator of the information value or not. To this end, the back-end will retrieve the creator of the intervention value from the database. In addition, it will extract the identity of the connected user using the user token. Those users are then compared. If the connected user is the creator of the information value, this value will be retrieved and returned to the user. However, if the user is not the creator of the information value, the read response will be set as Forbidden and returned to the front-end. In this case, the user will not have access to the requested information value.

The second algorithm, called Delete information value, aims at controlling the deletion of an information value by an end-user. Similarly to reading an information value, in order to delete an information value, a user should be authenticated, participates in the intervention in which the action is executed, and has the appropriate access right for deleting the information. However, an additional requirement is included in this case. In order to delete an information value, the user who executes this action must be the creator of this value. This will serve for reinforcing the access control mechanism. Algorithm 3 represents the algorithm for deleting information value. This algorithm is executed with each delete and transmit activity (Cf. Section 6.6.5). If this request is authorised, the information value will be deleted from the database. On the contrary, if the request is not authorised, a Forbidden response will be returned to the user. Inputs of this algorithm are the name of the group of information containing the information value to delete, the information name, the user token, and the id of target intervention based on the user's selection. Whereas the output is the delete response. Similarly to the read information algorithm, the first two tests

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

executed in the delete information value algorithm are user authentication and participation in the target intervention. If those two tests are passed, a new test will be executed to determine whether the connected user is the creator of the information value. If the connected user is not the creator of the information value, the delete response will be set as Forbidden and returned to the front-end. However, if the user is the creator, the back-end will continue to the next step

Algorithm 3: Delete information value

Input: Group of Information: Name of group of information, Information: String that represents the information name, User Token: Access Token containing the user id, Id of Target Intervention

Output: Delete Response: String

```
1 Initialization;
2 if User !Authenticated then
3   | Delete Response  $\leftarrow$  Forbidden;
4   | Redirection to Authentication page;
5 else
6   | if User's team  $\notin$  Intervention teams then
7     | Delete Response  $\leftarrow$  Forbidden;
8     | Return Delete Response;
9   | else
10    | Check if user is Creator(User Token, Information Value);
11    | if User  $\neq$  Creator then
12      | Delete Response  $\leftarrow$  Forbidden;
13      | Return Delete Response;
14    | else
15      | Action  $\leftarrow$  Delete;
16      | Retrieve Role from database(User Token);
17      | AccessType  $\leftarrow$  GetAccessType(Action, Group of Information, Role);
18      | if AccessType = Forbidden then
19        | Delete Response  $\leftarrow$  Forbidden;
20        | Return Delete Response;
21      | else
22        | Move Information Value to archive table;
23        | Delete Information Value from database;
24      | end
25    | end
26  | end
27 end
```

in the permission control mechanism. Hence, the access type will be determined based on the access right that the user's role has on the group of information containing the information value. Accordingly, the action will be set to delete and the SPARQL query that corresponds to the function *GetAccessType* will be executed. If the access type returned is Forbidden, the delete response will be set as Forbidden and the user's request will be rejected. However, if the access type is Authorized, the information value will be deleted. We notice that, in order to guarantee traceability of user's action, deleted information values are moved to an archive table before executing this deletion.

The third algorithm, as mentioned previously, serves for authorising or forbidding create and update actions. Permissions for these two actions are integrated in the same algorithm since the same requirements for both actions are identical. In order to create or update an information value, there exist only three requirements. The first requirement is that the user should be authenticated. The second requirement is that the user participates in the intervention in which the action is executed. Whereas the third requirement is that the user has the needed access right for creating or updating an information value. Algorithm 4 represents the algorithm for creating or updating information value. This algorithm is executed with each create and transmit activity (Cf. Section 6.6.5). If this request is authorised, the information value will be created or updated in the database. On the contrary, if the request is not authorised, a Forbidden response will be returned to the user. Inputs of this algorithm are the name of the group of information, the information name, the information value transmitted, the user token, and the id of target intervention based on the user's selection. Whereas the output is the create response. As we can see in algorithm 4, similarly to the algorithms 2 and 3, the first two tests executed in the create or update information value algorithm are user authentication and participation in the target intervention. If those two tests are passed, a new test will be executed to determine if the action is create or update. The main difference is that in the case of create, the user who executes the action should be inserted as the creator of the information value in the database. This will serve for policies of information deletion or retrieval as discussed in algorithms 2 and 3. Hence, the back-end will test if the information value transmitted already exists in the database. If the value does not exist, then the action is create. Accordingly, a SPARQL query will be executed on the knowledge base to determine the access type based on the create action, the group of information, and the role. In this case, if the returned response is Forbidden, the create response will be set as Forbidden and returned

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

Algorithm 4: Create or update information value

Input: Group of Information: Name of group of information, Informations: String that represents the information name, Information Value, User Token: Access Token containing the user id, Id of Target Intervention

Output: Create Response: String

```
1 Initialization;
2 if User !Authenticated then
3   | Create Response  $\leftarrow$  Forbidden;
4   | Redirection to Authentication page;
5 else
6   | if User's team  $\notin$  Intervention teams then
7     | Create Response  $\leftarrow$  Forbidden;
8     | Return Create Response;
9   | else
10    | if Information Value  $\nexists$  in database then
11      | Action  $\leftarrow$  Create;
12      | Retrieve Role from database(User Token);
13      | AccessType  $\leftarrow$  GetAccessType(Action, Group of Information, Role);
14      | if AccessType = Forbidden then
15        | Create Response  $\leftarrow$  Forbidden;
16        | Return Create Response;
17      | else
18        | Creator  $\leftarrow$  Retrieve user id(UserToken);
19        | Insert Creator & Information Value in database;
20      | end
21    | else
22      | Action  $\leftarrow$  Update;
23      | AccessType  $\leftarrow$  GetAccessType(Action, Group of Information, Role);
24      | if AccessType = Forbidden then
25        | Create Response  $\leftarrow$  Forbidden;
26        | Return Create Response;
27      | else
28        | Update Information Value in database;
29      | end
30    | end
31  | end
32 end
```

to the front-end. However, if the returned response is Authorized, the information value will be inserted in the database. In addition, the back-end will extract the identity of the connected user using the user token, set it as the creator of the information value and inserts it in the database. Regarding the update case, the same procedure will be applied. However, the information value creator will not be modified in the database.

6.6.4 Information reception and consulting

As it has been presented in 6.6.3.2, information reception and consulting activity is based on extracting information values of a certain group of information from the database. Accordingly, it corresponds to the read action and mainly follows the information transmission activity. Figure 6.29 shows a sequence diagram for information reception and consulting. As we can see in Figure 6.29, in order to retrieve information values of a specific group of information, a GET request is transmitted from the front to the back-end. This request contains the name of the group of information, the different information elements of the group, the intervention id retrieved from the selected intervention, and the user id retrieved from the authentication phase. Hence, for each information, a permission control test must be executed at the back-end in order to determine whether the read action is forbidden or authorized. For instance, the back-end will verify if the end-user is authenticated, participates in the target intervention, and has the read

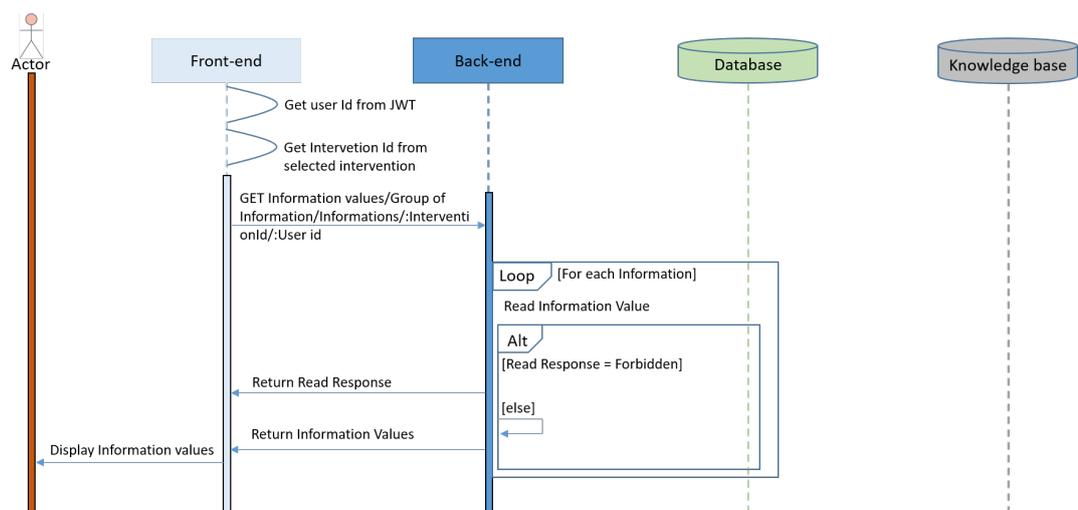


Figure 6.29: Sequence diagram for information reception and consulting.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

permission based on the read information value algorithm. If the read response returned is Forbidden, this response will be returned to the front-end and the end-user will not have access to information values. Otherwise, information values will be retrieved from the database and returned to the end-user through the front-end.

6.6.5 Transmission of information

Transmission of information is the second main communication activity to be achieved by the end-users. We recall that, in order to simplify the user's tasks, we propose to allow the user to transmit required groups of information as presented in the interaction model instead of transmitting each information element apart. Figure 6.30 shows a sequence diagram for information transmission. As we can see in Figure 6.30, two main actions can be achieved by the user in this context that are: Delete, or Create and transmit. When the user deletes a group of information, a DELETE request will be transmitted from the front to the back-end. This request contains the name of the group of information, the different

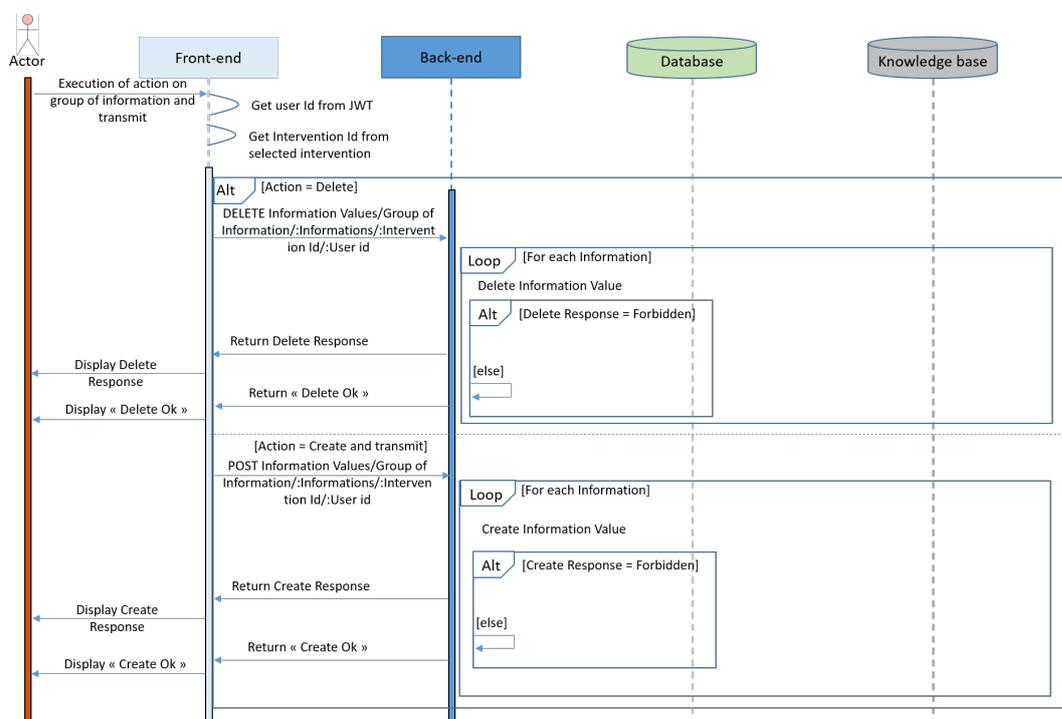


Figure 6.30: Sequence diagram for information transmission.

information elements of the group, the intervention id retrieved from the selected intervention, and the user id retrieved from the authentication phase. Therefore, for each information, a permission control test must be executed at the back-end in order to determine whether the delete action is forbidden or authorized based on the delete information value algorithm. If the delete response is Forbidden, this response will be returned to the front-end and the user will not be able to delete the information values. Otherwise, the information value will be deleted from the database and a notification of this deletion will be displayed to the user. Regarding the information creation and transmission activity, when the user creates or updates and transmits a group of information, a POST request will be transmitted from the front to the back-end. This request contains the name of the group of information, the different information elements of the group and the information values, the intervention id retrieved from the selected intervention, as well as the user id retrieved from the authentication phase. Therefore, for each information, a permission control test must be executed at the back-end in order to determine whether the create or update action is forbidden or authorized based on the create or update information value algorithm. If the create response is Forbidden, this response will be returned to the front-end and the information values will not be created nor updated in the database. Otherwise, information values will be either created or updated in the database and a creation notification is returned to the end-user.

We notice that we have two ways for processing the groups of information in terms of visualisation, transmission, and reception based on the nature of the group of information. For some groups of information, the end-users should have the ability to create, transmit, and visualise different instances of the group even in a single intervention. Those groups are *Medical Record*, *Actor To Involve*, *Material To Engage*, *Centre To Engage*, *Engaged Material*, *Victims General Information*, *Unavailable Material*, *Unavailable Actor*, *Achieved Tasks*, *Current Tasks*, *Requests for Material*, *Requests for Actor*, and *Commander Decisions Information*. For instance, different actors are involved in a rescue intervention. Therefore, the CTA Operator should be able different instances of the group actor to engage. Moreover, several medical records that belong to different victims may be fulfilled and exchanged during a single intervention. Hence, in order to differentiate those records, we propose to refer to each medical record using a unique id. In addition, in order to give the users the possibility of consulting different medical records, we propose to illustrate the totality of records that belong to an intervention on the user's interface. The totality of those records are illustrated in the same

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

way on the basis of the configuration of specifications step. Whereas, for other groups of information, these groups are created only once during an intervention. In this context, the end-users should have the ability to fulfil, transmit, and visualise those groups without the need for creating new instances of the group. Examples of those group are *Incident Information*, *Intervention Site General Information*, and *Intervention Site Accessibility Information*. For instance, the group intervention site general information is created only once and can be then updated and transmitted as much as required. Regardless of the nature of the group, the permissions control mechanism is identical in those two cases. We also notice that the groups Centres Cartography, Persons Cartography, Material Cartography, and Hospitalisation Centres Availability Information are generally intervention independent and differ from the other groups in terms of design and consulting. However, in this work, we do not consider the special case of those four groups.

6.7 Discussion

In this chapter, we proposed a design platform that allows final users to design system interfaces and specifications in a customised way. The proposed platform guarantees the confidentiality of information and is mainly based on the interaction model presented in Chapter 4 and ResOnt ontology presented in Chapter 5. MODES platform responds to four out of five stakeholders' needs that were identified in Chapter 2 as shown in table 6.2. Moreover, as we can see in table 6.3, three out of four criteria that an efficient communication system oriented to rescue operations must meet, are fulfilled in MODES.

6.8 Conclusions

The main objective of this thesis focus on proposing an approach for designing a communication system that aims at supporting situation awareness in rescue operations. The third step in the proposed approach lies within the conception and development of a design platform. Whereas the fourth step consists in integrating confidentiality mechanisms in order to guarantee confidential access to information in the final system. Accordingly, as the third and fourth steps, we proposed a design platform that allows final users to design system interfaces and

Table 6.2: Comparison of MODES to other existing systems according to stakeholder' needs.

Need	System										
	1	2	3	4	5	6	7	8	9	10	11
Exchange of actionable information based on context	X			X		X	X		X	X	X
Common terminology			X	X	X	X	X		X	X	X
Interoperable communications between all the services	X		X	X	X	X	X		X	X	X
Exchange of different required types and forms of information	X	X							X	X	X
Resources allocation	X	X		X				X	X	X	

1:MIKoBOS [Meissner *et al.*, 2006]2:MobileMap + DDSS [Monares *et al.*, 2011a,b]3:MoRep [Ludwig *et al.*, 2013]4:SHARE [Konstantopoulos *et al.*, 2006, 2008; Velde *et al.*, 2005]5:Communicating Ambulance [Mallek *et al.*, 2016]

6:Nomadeec + Nomadeec Telexpert [Nomadeec France, 2019]

7:SINUS + ArcSINUS [Séguret, 2013]

8:Pilot Mobile [TplSystemes France, 2019]

9:POLARISC [Elmhahbi, 2020]

10:NexSIS [Lambert *et al.*, 2019]

11:MODES

specifications in a customised way. The proposed platform guarantees the confidentiality of information and is mainly based on the interaction model presented in Chapter 4 and ResOnt ontology presented in Chapter 5.

Thanks to MODES platform, final users will be able to define the specifications of the system. In addition, each user will be able to design her/his graphical interface in a customised way based on her/his context. According to specifications and design, end-users will be able to connect to the final system in order to exchange information in rescue operations. In this chapter, we described the basic principles and requirements for designing a communication system by its-end users based on their contexts. We then presented the architecture of the proposed platform. Afterwards, we discussed the main functionalities needed and implemented to meet those requirements. Furthermore, we proposed an access control

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

Table 6.3: Comparison of MODES to other existing systems according to the criteria for an effective communication system.

System \ Criterion	System											
	1	2	3	4	5	6	7	8	9	10	11	
Taking into account the diversity of stakeholders' needs									X	X		
Personalisation and adaptability to users' contexts	X			X		X	X		X	X	X	
Flexibility	X			X	X				X	?	X	
Confidentiality			X	X	X	X	X	X		X	X	

1:MIKoBOS [Meissner *et al.*, 2006]

2:MobileMap + DDSS [Monares *et al.*, 2011a,b]

3:MoRep [Ludwig *et al.*, 2013]

4:SHARE [Konstantopoulos *et al.*, 2006, 2008; Velde *et al.*, 2005]

5:Communicating Ambulance [Mallek *et al.*, 2016]

6:Nomadeec + Nomadeec Telexpert [Nomadeec France, 2019]

7:SINUS + AreSINUS [Séguret, 2013]

8:Pilot Mobile [TplSystemes France, 2019]

9:POLARISC [Elmhahbi, 2020]

10:NexSIS [Lambert *et al.*, 2019]

11:MODES

and rights management policy integrated into the system. In this context, we adapted and modified the TT-RBAC model in order to enforce the information confidentiality in the system.

After having modelled interactions, created an application ontology, and presented the design and communication platform, we move to the last step that consists in designing the communication system by its end-users and exchanging information through this system. To this end, we have developed the proposed platform by taking into account different specifications described in this chapter. In the next chapter, we show the relevance of our assumptions based on the implementation of the platform. Unfortunately, in this thesis, we did not have the opportunity to test the proposed platform by its end-users. Accordingly, we propose to test it by our-self in order to validate its main functionalities. To this end, we present, in the next chapter, a design and communication exchange scenario based on a part of the interaction model presented in Chapter 4. This scenario

will serve to validate our results and conclude the limitations of this work.

6. A NEW SECURED PLATFORM FOR RESCUE SITUATION AWARENESS AND COMMUNICATIONS

Chapter 7

Experimentations

Contents

7.1	Introduction	220
7.2	Platform Implementation	220
7.3	System Design	227
7.3.1	Configuration of specifications	227
7.3.2	Design and templates creation	230
7.4	Scenario of incident	238
7.4.1	Scenario description	238
7.4.2	Communication based on the scenario described	239
7.5	Conclusions	246

7.1 Introduction

In this thesis, we proposed an approach for designing a communication system that aims at supporting situation awareness and communications in rescue operations. The aforementioned approach consists of a five-step methodology. In Chapter 4, we presented the first step of the proposed approach that consists in modelling interactions and communications in these operations. The result of this first step is an interaction model that illustrates different practices of rescue actors involved in French rescue operations and interactions between them. Afterwards, in Chapter 5, we presented the second step that requires building an application ontology. The result of this step is an ontology called ResOnt that represents the knowledge required for designing a communication and awareness-support system oriented for rescue actors that guarantees the confidentiality of information. Then, in Chapter 6, we presented the third and fourth steps of the proposed approach. The third step consists in designing a platform that allows the dynamic configuration and customised design of the system's interfaces. Whereas the fourth step relies on integrating confidentiality mechanisms in order to guarantee confidential access to information in the final system. The result of those two steps is a customised communication system that guarantees information privacy. In order to show the relevance of our assumptions, we have developed the conceived platform on the basis of the specifications described in Chapter 6. In this chapter, we present an overview of different technologies used in the platform implementation. Moreover, we present distinct functionalities included in the platform. Afterwards, we present a case of using the proposed platform. Hence, we design different interfaces for multiple users and configure different specifications. Then, we describe a communication scenario using the platform in the case of a road accident. This scenario will serve to validate our results and conclude the limitations of this work.

7.2 Platform Implementation

Based on the architecture and functionalities presented in Chapter 6, we have developed a test platform in order to prove the feasibility and usability of this latter. In Chapter 6, different components required in the platform were presented. Hence, we have integrated those components and used adopted technologies as follows:

- **Front-end:** In order to develop the front-end part, we used ReactJS. ReactJS is a free JavaScript library developed by Facebook. It serves for the creation of web applications using the concept of a component. Components allow the user interface to be divided into independent and reusable elements, enabling each element to be considered in isolation. A visible page in a user interface is a component or is made up of several components. Although today's JavaScript engines are fast enough to handle complex applications, Document Object Models (DOM) manipulations are still not that fast. React solves this problem by using something called virtual DOM that is stored in memory.
- **Knowledge base and inference engine:** Regarding the knowledge base, we first used protégé software to develop the ontology in owl. Then, we used the Jena Fuseki server [Jena, 2014] to store the Ontology. Jena Fuseki server is a SPARQL server implemented and employed by Apache. Jena-fuseki allows the conversion of the owl-2 ontology into a SPARQL database that could be queried using the SPARQL language [Harris *et al.*, 2013]. The reason behind choosing Jena Fuseki server is that it includes an inference engine that allows querying the ontology. In addition, thanks to the Fuseki server, the knowledge base can be queried in any application using a package called Sparql-http-client. The latter allows performing SPARQL queries on a SPARQL database through the HTTP protocol.
- **Back-end and Database:** To develop the back-end part, we used Strapi. Strapi is a flexible, open-source Headless Content Management System (CMS). It offers the possibility of the simple creation of REST APIs. Moreover, it offers a back office that includes a graphical interface. This latter allows a simple managing of database tables, as well as stored values. Regarding the database, Strapi supports PostgreSQL, MongoDB, SQLite, MySQL and MariaDB. Accordingly, we used SQLite since it is the recommended database to quickly create an application locally.

Figure 7.1 illustrates the main components and the used technologies in the developed platform. As we can see in Figure 7.1 and mentioned in Chapter 6, requests between the front-end and the back-end use the HTTP protocol. Those requests are handled in the back-end and then executed on the relevant destination either on the database or on the knowledge base through the Fuseki server. Regardless of the type of the query, the query results are returned to the back-end that

7. EXPERIMENTATIONS

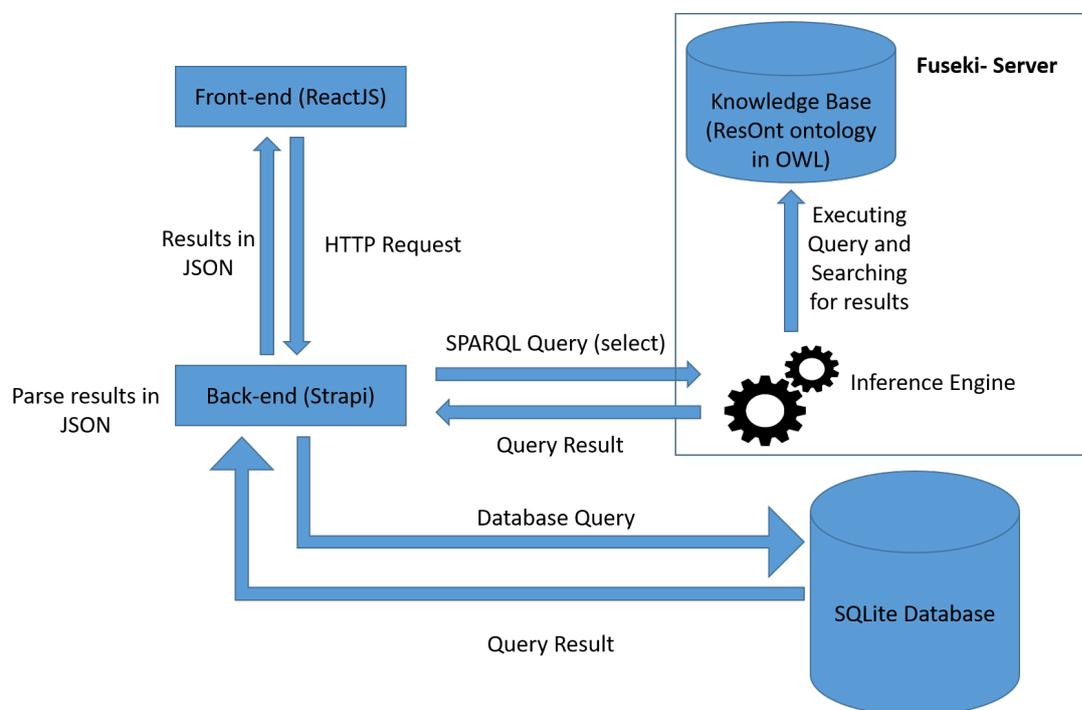


Figure 7.1: Components and technologies in the developed platform.

handles the results. Those results are then parsed into JSON and returned back to the front-end. As it has been presented in 6.3.1, different functionalities are required in the proposed solution. Hence, we have developed and integrated multiple functionalities to obtain a useful solution that meets the basic principles. Those functionalities are:

- Connexion and login to the application: Thanks to this functionality, end-users will be able to connect and login using their credentials. Accordingly, we have integrated the required module and interface for users' login.
- Creation of context and configuration of context elements: This will allow end-users to create different contexts based on operational practices. Moreover, it enables the configuration of context elements that are Phase, Sub-phase, Location, and Communication instrument by selecting specific values through a set of proposed values for each element. To this end, we have implemented the required functions that allow the retrieval of the possible values for each element from the knowledge base. In addition, necessary functions to store the contexts created in the database were integrated

into the platform.

- Creation and configuration of tasks in a given context: Thanks to this functionality, end-users are allowed to check different tasks associated with their roles on the basis of their context. In addition, those users are able to check and delete, if required, the groups of information and information elements required or used by each task. To this end, we have integrated several functions that retrieve the user's tasks from the knowledge base. In addition, different functions needed for retrieving different groups of information and their information elements were integrated into the platform. Moreover, we have integrated the required mechanisms for deleting a group of information or an information element from a given context as well as mechanisms needed to store tasks, groups of information, and information elements in the database for further retrieval.
- Configuration of the system specifications and information properties based on a set of proposed properties and possible values: Thanks to this functionality, the system's administrators are able to configure the specifications in a dynamic way by assigning specific values to several parameters. To this end, we have implemented and integrated the necessary functions to retrieve different groups of information, their information elements, and distinct properties related to information. Those functions will also ensure retrieving the sets of possible values per property. Moreover, we have included the required functions that allow storing the administrator's choices in the database for further retrieval. Besides, different functions required for generating interfaces and the system's specifications on the basis of properties' values were integrated into the platform developed. We would like to recall that, in this thesis, we only consider the informational component and the field type among different properties.
- Creation of personalised templates related to contexts and users identities: This functionality allows end-users to create a template per context. It also serves for adapting the template's size to the instrument's interface. On the basis of the selected context, the end-user can visualise different groups of information and their information elements in the right informational component. We notice that those components are integrated into a template based on the configuration of specifications. Accordingly, different functions required for retrieving the contextual groups of information

7. EXPERIMENTATIONS

and their elements were integrated into the developed platform. In addition, functions required for retrieving possible values of information upon requirements were developed and integrated into the platform. Furthermore, functions required for generating responsive interfaces were included in the platform developed. Two categories of interfaces are considered in this context: (1) Large interfaces such as desktops', laptops', and tablets' interfaces; and (2) small interfaces such as those of smartphones.

- Integration of required media components to the created templates: Thanks to this functionality, the end-user is allowed to integrate multiple media components in a created template upon requirement. Hence, we have developed several functions required for retrieving the possible media components from the ontology ResOnt. In addition, functions needed for integrating the right media component on the basis of the user's selection were included in the developed platform. We would like to remember that, in this work, we only consider output media components.
- Positioning of different informational and media components in created templates: Thanks to this functionality, the end-users are able to change the position of different groups of information in a created template. In addition, they are allowed to change the positions of media components integrated into that template. We would like to remind that there exist two cases for information positioning. The second case is applied for contexts that are based on the usage of smartphones. In this case, the end-users are able to change the order of different components while respecting the limitations of a smartphone interface. By changing this order, the position of the group of information will be modified. We notice that, in this case, no more than two components can be placed together horizontally at the same line in order to respect the borders' limitations. To this end, we have used the grid functions of material design. On the other hand, the second case is applied for contexts that contain a Desktop, Laptop, or Tablet as a communication instrument. In this case, the users will be able to change the positions of components in different ways and multiple components can be placed horizontally at the same line. To this end, we have used the drag and drop functions of ReactJS together with the grid functions of material design. In this context, the end-user can change the position either using the drag functions or by changing the groups' orders. Eventually, we have

implemented the required functions for storing created templates in the database for further retrieval.

- **Connexion to intervention and context selection:** In this context, through the developed platform, the end-users are able to connect to intervention through a set of created interventions. In addition, those users are able to select their context in the intervention. On the basis of this selection, the adequate template will be retrieved and displayed to the user. To this end, we have integrated the required functions and interfaces for retrieving the sets of interventions and contexts and displaying those latter to the users. In addition, functions required for extracting the appropriate template from the database on the basis of the user's selection were developed and integrated into the platform.
- **Creation, transmission, reception, and visualisation of information:** Thanks to those functionalities, the end-users are able to communicate with each others after being connected to intervention. In this context, they are able to transmit, receive, and visualise different groups of information. We would like to remember that there exist two ways for processing the groups of information in terms of visualisation, transmission, and reception based on the nature of the group of information. For some groups of information, the end-users are able to create, transmit, and visualise different instances of the group even in a single intervention. For instance, several medical records that belong to different victims can be created, fulfilled, and exchanged during a single intervention. Whereas, for other groups of information, these groups are created only once during an intervention. In this context, the end-users are able to fulfil, transmit, and visualise those groups without the need for creating new instances of the group. For instance, the group intervention site general information is created only once and can be then updated and transmitted upon requirements. To this end, for each group of information, we have added different interface components required for the transmission and deletion of the group. In this context, we have added a button for transmission and a button for deletion per group. Moreover, regarding the groups that belong to the first category, we have added a button that serve for creating multiple instances of the group. Besides, different functions required for storing and retrieving different groups of information as well as information and values of distinct groups in the database were also developed and integrated into the platform.

7. EXPERIMENTATIONS

In addition to those functionalities, we have implemented and integrated several mechanisms and tests required for obtaining a functional communication system that responds to the basic principles. Those mechanisms are:

- **User Authentication:** In order to retrieve users' identities and forbid any external access, ensuring users' authentication is required in the system. Accordingly, we have integrated an authentication mechanism based on the JSON Web Token (JWT). In addition, different functions required for retrieving users' identities based on the authentication mechanism were also integrated into the platform.
- **Rights Management and Permissions Control:** In order to control access to information in the system, an access control policy and rights management policy was proposed in Chapter 6 on the basis of an adaptation of TT-RBAC model. This policy consists of rights management and permissions control. Accordingly, we have defined different access rights. In addition, we have identified the required mechanisms and functions required for controlling different permissions. Those functions were also implemented and integrated into the developed platform.

After having developed the proposed platform, it is necessary to test it in order to evaluate it. As stated in Chapter 6, in this thesis, we did not have the opportunity to test the developed platform by its end-users. Accordingly, we propose to test it by our-self in order to validate the implemented functionalities. To this end, we present, in the next section, a design example through which we design different interfaces for multiple users and configure different specifications. Then, in section 7.4, we present a scenario of communication using the platform following a road accident. In order to ease the navigation in the platform, we created a menu with three modules as shown in Figure 7.2. The first module called *Configure Specification* serves for configuring specifications. The second module entitled *Design Interface* allows creating different contexts and personalised templates. Whereas, the third module called the *Final system* allows selecting and connecting to intervention as well as exchanging and visualising information.

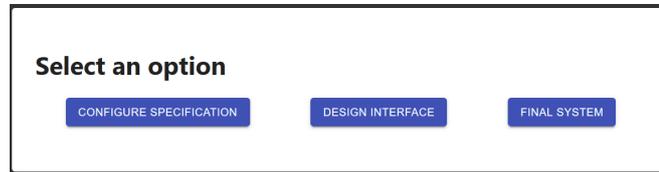


Figure 7.2: Three created modules in the developed platform.

7.3 System Design

As it has been discussed in Chapter 6, the system’s design consists of two main activities. The first one, which is of responsibility of the system’s administrator, consists in configuring different specifications of information elements. On the other hand, the second activity consists in designing customised graphical interfaces by the end-users. Hence, in 7.3.1, we start with an example of configuring specifications for several information elements. Then, in 7.3.2, we design different graphical interfaces for multiple users having different contexts.

7.3.1 Configuration of specifications

This activity consists in identifying the specifications of information elements for each group of information created in the system. In this context, for each and every property that belongs to an information element, we select a specific value from a set of possible values. We would like to remember that the properties considered in this thesis are the informational component and the field type. Hence, we will not configure other properties that were not considered. Moreover, the configuration of specifications is identical to all the information elements that belong to all the groups of information. Therefore, to avoid repetition, we will show the example of configuration of information elements that belong to a single group of information entitled *Incident Information*.

As we can see in Figure 4.8, the aforementioned group has three information elements respectively *Incident* that represents the type of the incident, *Address* that represents the address of the incident, and *Time* that represents the date and time of the incident. Accordingly, in the configuration of specifications section, those information elements as well as their properties and possible values are retrieved and displayed. Figures 7.3, 7.4, 7.5, 7.6, and 7.7 illustrate the configuration of the three information elements *Address*, *Incident*, and *Time* of the group *Incident Information* respectively. As we can see in Figure 7.3, the possible values

7. EXPERIMENTATIONS

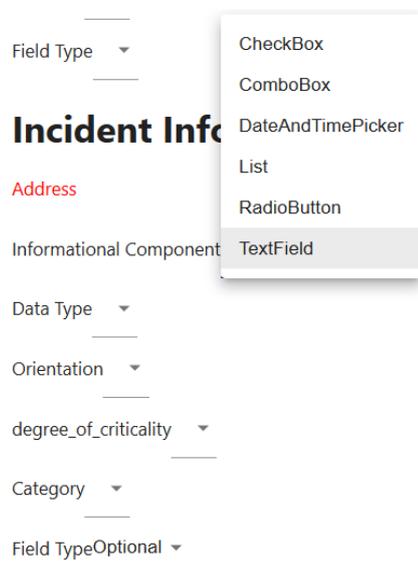


Figure 7.3: Possible values of the informational components in the platform.

for the informational component are: Text box, combo box, radio button, list, checkbox, and date and time picker. On the other hand, for the field type, two possible values are proposed. Those values are Obligatory and Optional as shown in Figure 7.4. Accordingly, regarding the *Address*, since it cannot be predicted in advance, we select *Text box* as the *Informational component* and *Optional* as the *Field type* as illustrated in Figure 7.5. For the element entitled *Incident*, since

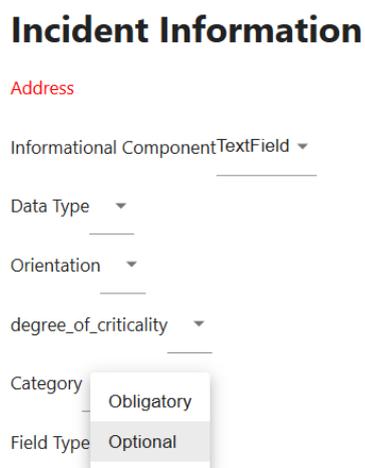


Figure 7.4: Possible values of the field type in the platform.

The screenshot shows a configuration window titled "Incident Information". Under the heading "Address", there are several dropdown menus for configuration: "Informational Component" is set to "TextField", "Data Type" is empty, "Orientation" is empty, "degree_of_criticality" is empty, "Category" is empty, and "Field Type" is set to "Optional".

Figure 7.5: Configuration of specifications for the information entitled *Address*.

its possible values are previously defined in ResOnt ontology, we select *ComboBox* as the *Informational component* and *Obligatory* as the *Field type* as shown in Figure 7.6. Regarding the *Time*, we choose *Date and Time Picker* as the *Informational component* and we set the *Field type* to *Optional* as illustrated in Figure 7.7. After having configured the specifications of different information elements that belong to the totality of the groups of information, we move to the design and creation of customised templates.

The screenshot shows a configuration window titled "Incident Information". Under the heading "Incident", there are several dropdown menus for configuration: "Informational Component" is set to "ComboBox", "Data Type" is empty, "Orientation" is empty, "degree_of_criticality" is empty, "Category" is empty, and "Field Type" is set to "Obligatory".

Figure 7.6: Configuration of specifications for the information entitled *Incident*.

7. EXPERIMENTATIONS

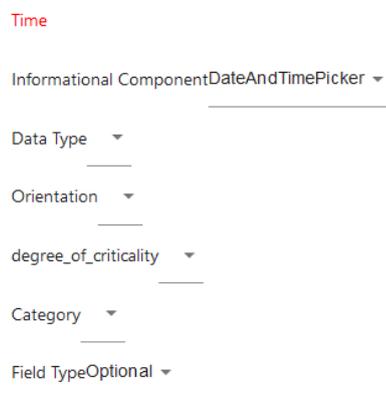


Figure 7.7: Configuration of specifications for the information entitled *Time*.

7.3.2 Design and templates creation

As stated in chapter 6, the design of customised interfaces consists of two activities that are context identification and template creation. The first activity requires creating the context, configuring the different elements it is made of, and creating different tasks associated with the context. Regarding the second activity, it consists in creating a customised template for each identified context, integrating different media components, and positioning different informational and media components on the created template. The end-user will then select her/his context in the intervention in order to retrieve the corresponding template and communication with other users. In chapter 4, we showed that different organisation members with distinct roles participate in a rescue operation. Each of those members may have one or several contexts in an operation depending on her/his role. Accordingly, one must create a single template per context. Given that the context identification and templates creation are identical to different end-users, we will not create contexts and templates for the totality of organisation member roles. Accordingly, in this example, we only consider three organisation members that have three roles respectively: *CTA Operator*, *CIS Operator*, and *Commander of Rescue operation*. In addition, to simplify the visualisation of the created templates, we will not create each and every task in each and every context. However, in practical operations, one must configure all the tasks in order to determine the required information in that context. Furthermore, in this example, we only consider the first two phases of a rescue operation respectively: *Alert Phase*, and *Involvement of required resources*. For demonstration purposes, for each organisation member role stated above, we will create different contexts

on the basis of those two phases.

By referring to the interaction model presented in Chapter 4, specifically Figures 4.8, 4.9, and 4.10, we can see that the Alert phase has a single sub-phase entitled *Alert Reception and Processing* with a single participating role, which is the *CTA Operator*. On the other hand, the *Involvement of required resources* has four sub-phases respectively: *Reception of departure ticket in CIS*, *Confirmation to CTA*, *Warning rescuers*, and *Verification of resources and preparation for departure*. In this example, we only consider the first and the third sub-phases of the latter phase. Hence, we do not consider the confirmation to the CTA nor the preparation for departure. As we can see in Figure 4.9, the sub-phase entitled *Reception of Departure Ticket* has a single participating role, which is the *CIS Operator*. Regarding the third sub-phase, entitled *Warning rescuers*, it involves the participation of the *CIS Operator* as well as the *Rescuers* represented by the *Commander of rescue operation*, the *sappers*, and the *driver*. Figure 7.8 illustrates the phases of a rescue operation. In this figure, the two phases as well as their sub-phases considered in the design and communication example are highlighted in red. In addition, we highlight in this figure the organisation member roles that are taken into consideration in the present example. Accordingly, we have created three users in the database. The first user has the role of Commander of rescue operation. The second user is a CTA Operator. The third user has the role of CIS Operator. In the following, we will create and configure different contexts and templates for each of the users identified based on their participation in the two selected phases.

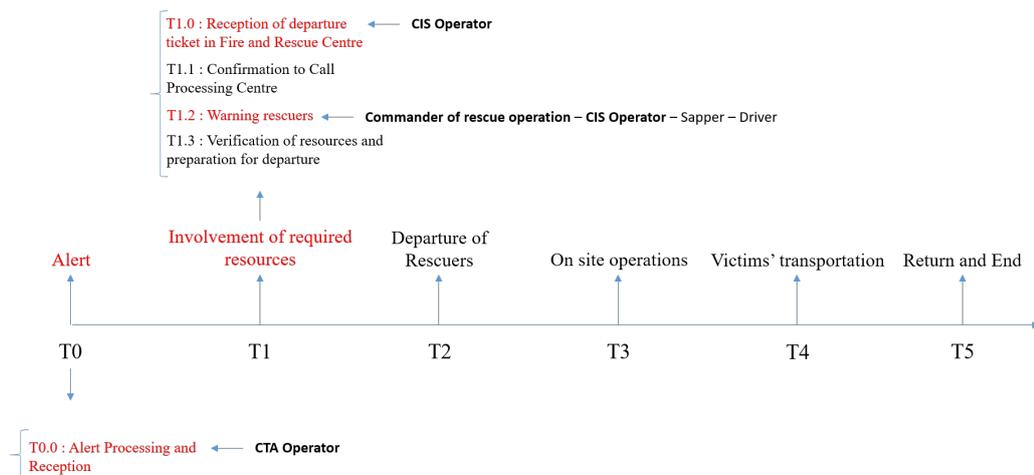


Figure 7.8: Phases, sub-phases, and roles considered in the example.

7. EXPERIMENTATIONS

7.3.2.1 Case of Commander of rescue operation

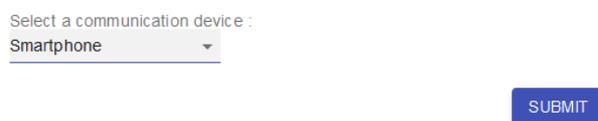
As discussed in 7.3.2 and illustrated in Figure 4.9, in this example, the *Commander of rescue operation*, so-called the CRO, is only involved in the sub-phase entitled *Warning rescuers* of the phase called *Involvement of required resources*. During this sub-phase, the CRO exists in the CIS and may use either a smartphone or a tablet. In this example, we consider the case of a *Smartphone*. Accordingly, in this example, the CRO has a single context with a single task: *Reception of departure ticket by rescuers*. Accordingly, we created the aforementioned context and task as shown in Figures 7.9, 7.10, and 7.11 respectively. After having created the context and the user's task, we move to the creation of a template for this user. By referring to Figure 4.9, we notice that the task entitled *Reception of departure ticket by rescuers* requires the seven groups that compose the departure ticket: *Incident Information*, *Intervention Site General Information*, *Intervention Site Accessibility Information*, *Victims General Information*, *Material to engage*, *Actor to involve*, and *Specific dangers*. Hence, those groups and



Give a name to the context :
Context 1 CRO
Phase :
Involvement Of Requir...
Sub Phase :
Warning Rescuers
Location :
Fire And Rescue Centre

SUBMIT

Figure 7.9: Configuration of context elements for a CRO.



Select a communication device :
Smartphone

SUBMIT

Figure 7.10: Selection of Smartphone in a context for CRO.



Reception Of Departure Ticket By Rescuers

SUBMIT

Figure 7.11: Creation of task associated with CRO.

information elements are located with the right components on the template as we can see in Figure 7.12 that illustrates a partial view of the initial template created for the CRO. As it has been discussed in Chapter 6 and illustrated in Figure 7.12, in the case of a smartphone, the template's size is adapted to the device interface and no more than two groups of information are located at the same level horizontally. The positions of different groups of information can be modified by changing the order of each group on the template. Hence, we modified the orders of those groups and obtained a customised template as shown in Figure 7.13. This template will be retrieved and visualised by the user during the connexion to intervention for communication and exchange of information.

7.3.2.2 Case of CTA Operator

As discussed in 7.3.2 and illustrated in Figure 4.8, in this example, the participation of the CTA Operator is limited to the phase entitled *Alert phase*, which has a unique sub-phase called *Alert Reception and Processing*. During this sub-phase, the CTA Operator exists in the call processing centre and can use either a Laptop or a Desktop for communicating. In this example, we consider the case of a *Desktop*. In addition, during this sub-phase, the *CTA Operator* has four associated roles that produce or require information respectively: *Fulfilment of call information in the system*, *Cartography consulting*, *Selection of resources*, and *Fulfilment and transmission of departure ticket to CIS Operator*. In this example,

Figure 7.12: Partial view of the template created for the CRO before modification.

7. EXPERIMENTATIONS

Figure 7.13 shows a partial view of a final template designed for the CRO. The template is organized into five distinct sections, each with a title and a dropdown menu for reordering:

- Intervention Site General Information (3):** Includes a dropdown for SiteFunction, a dropdown for SiteType, and two checkboxes: Private Place and Public Place.
- Intervention Site Accessibility Information (4):** Includes input fields for RoadToTake, Address, Distance, and TimeToArrive.
- Specific Dangers (5):** Includes input fields for Danger and Localisation.
- Material To Engage (6):** Includes a dropdown for Material and an input field for ID.
- Victims General Information (7):** A section for victim information.

Figure 7.13: Partial view of final template designed for the CRO.

we only consider two tasks in order to simplify the visualisation of the created template. Accordingly, we have created the context of CTA Operator by selecting the *Alert phase* as the intervention phase, the *Alert Reception and Processing* as a sub-phase, and the *CTA* as Location. In addition, we selected the *Desktop* as the communication instrument. Afterwards, we created the two aforementioned tasks as shown in Figure 7.14. After having created the context and the user's tasks, we move to the creation of a template for this user. By referring to Figure 4.8, we notice that the task entitled *Fulfilment of call information in the system* produces five groups respectively: *Incident Information*, *Intervention Site General Information*, *Victims General Information*, and *Specific dangers*. On the other hand, the second created task entitled *Fulfilment and transmission of departure ticket to CIS Operator* produces those groups as well as three other groups respectively *Material to engage*, *Intervention Site Accessibility Information*, and *Actor to involve*. We would also like to remind that, for each group of information produced or required by different tasks in the same context, this group is illustrated only once on the user's template in order to avoid repetition. Those groups and information elements are located with the right components on the template as we can see in Figure 7.15 that illustrates a partial view of the initial template created for the CTA Operator. As it has been discussed in Chapter 6 and illustrated in Figure 7.15, in the case of using a desktop, tablet, or laptop, the positions of different groups of information can be modified either by changing the order of each group on the template or by moving the group manually using the drag and drop functions. Therefore, we modified the orders of those groups and obtained a customised template as shown in Figure 7.16. This template will

Context 1 CTA Operator

Informations :

Phase : AlertPhase

Sub Phase : AlertReceptionAndProcessing

Location : CallProcessingCentre

Role : CTAOperator

Tasks :

Fulfilment Of Call Information In The System

Fulfilment And Transmission Of Departure Ticket

[CREATE TASK](#) [INFORMATIONS SUMMARY](#)

Template

Figure 7.14: Context and tasks created for the CTA Operator.

be then retrieved and visualised by the user during the connexion to intervention for communication and exchange of information.

7.3.2.3 Case of CIS Operator

As discussed in 7.3.2 and illustrated in Figure 4.9, in this example, the *CIS Operator* participates in two sub-phases of the phase called *Involvement of required resources*. The first sub-phase is called *Reception of departure ticket in CIS* while the second sub-phase is entitled *Warning rescuers*. As we can see in Figure 4.9, during those sub-phases, the CIS Operator exists in the CIS and may use either a desktop or a laptop. In this example, we consider the case of a *Desktop*. Hence, in this example, the CRO has two contexts each with a single task. Those tasks use the groups that compose the departure ticket. Accordingly, we created the aforementioned contexts and tasks following the same procedure adopted in 7.3.2.1 and 7.3.2.2. Moreover, for each created context, we created and designed a customised template as shown in Figures 7.17 and 7.18 respectively. In this section, we showed the effectiveness of the developed platform for configuring the system

7. EXPERIMENTATIONS

Material To Engage 7 6

Material * :
ID :
Distance :
TimeToArrive :
Health Care Facility Unit
Police
Name :
AgentFunction :
Professional
Volunteer
Skills :
ID :
Mature
Old
Young
Gravity :

Figure 7.15: Template created for the CTO Operator before modification.

Intervention Site General Information 2
SiteFunction * :
SiteType :
Private Place
Public Place

Intervention Site Accessibility Information 6
RoadToTake :
Address :
Distance :
TimeToArrive :

Specific Dangers 3
Danger * :
Localisation :

Victims General Information 4
VictimStatus :
Absolute Emergency
Dead
Good
Relative Emergency
Localisation :
Name :
Sex :
Female
Male
Age :
AgeRange :
Child
Mature
Old
Young
Gravity :

Actor To Involve 5
OrganizationMemberRole :
Affiliation :
Firefighters
Medical Services
Health Care Facility Unit
Police
Name :
AgentFunction :
Professional
Volunteer
Skills :
ID :

Incident Information 1
Incident :
Address :
Time :
November 17th 04:15 p.
Invalid Date Format

Material To Engage 7
Material * :
ID :

Figure 7.16: Final template designed for the CTA Operator.

Figure 7.17: Template designed for the CIS Operator during the sub-phase *Reception of departure ticket in CIS*.

Figure 7.18: Template designed for the CIS Operator during the sub-phase *Warning rescuers*.

specifications and designing customised interfaces in a flexible way. To this end, we configured the system's specifications and we showed how different templates are generated on the basis of those specifications. In addition, we created several templates for three users with different contexts. Based on the contexts, we

7. EXPERIMENTATIONS

illustrated the broad adaptation and customisation of those templates for each user.

7.4 Scenario of incident

After having tested the developed platform for designing the graphical interfaces in a customised way, we will assess its functionalities related to communication. To this end, we will describe a fictitious case of a road accident. We will then illustrate an example of information exchange during this accident using the developed platform.

7.4.1 Scenario description

On October 3rd, 2020 at 12:05 pm, a witness called the firefighters declaring a road accident and asking for firefighters intervention. This call was transmitted to the call processing centre (CTA) of Aube department based on the witness location. On the basis of the incident described by the witness, this incident occurred on October 3rd, 2020 at 11:58 am. It took place between two cars and a fuel truck on the main road “D 206” in Troyes city in France. This accident caused leakage of a large amount of fuel on the right side of the road. In addition, two victims were injured due to this accident. The first victim, Alex DUPONT, is a male child and has 8 years old. Alex was slightly injured, his status was good, and he was located in a black car with plate number “RT123456”. On the other hand, the second victim, Marine DUMOULIN, was a mature woman at the age of 46 years old. Unfortunately, Marine was severely injured and her status was classified as an absolute emergency. She was driving the second red car with plate number “AB456789”. During this intervention, only the second victim, Marine, was evacuated to a hospitalisation centre. Based on the nature of the accident, the number of victims, and the available material, the CTO Operator decided to engage the fire and rescue centre of Troyes that is 1Km far from the incident. Regarding the resources, he engaged one Road rescue vehicle with a plate number: “FF98764” as well as a rescue and assistance vehicle having “FF654123” as plate number. In addition, this operator involved four actors affiliated with firefighters in the intervention. The first actor, Jean, is a volunteer driver and rescuer with the personal ID “Vol543”. The second actor, Pierre, is also a volunteer rescuer and driver with the personal ID “Vol567”. The third and fourth actors are a

commander of rescue operation and a sapper respectively. The CRO, Olivier, is a professional firefighter. He has a unique ID “Pro683”. Regarding the sapper, Michael, he is a professional firefighter also with the ID “Pro790”.

7.4.2 Communication based on the scenario described

As stated in chapter 6, the communication through the developed platform consists of three activities that are: (1) Connexion to intervention and context selection; (2) Information reception and consulting; and (3) Transmission of information. Accordingly, in order to communicate using the designed system, the system’s administrator must create an intervention, assign different teams to the intervention as well as the required actors with those teams. In addition, the end-users should connect to the intervention based on their involvement. To this end, we created an intervention entitled *Intervention1* as well as a team called *Team1*. In addition, we assigned this team and intervention together. The three created users presented in 7.3.2 were also assigned to the *team1*. The importance of those assignments is to ensure the ability for controlling different permissions in the system as described in Chapter 6. We notice that, in this work, we do not take the receiver of each message into consideration since we are in the early development phases. In other words, when a user transmits information, it is automatically and simultaneously accessed by different users that have the right to this access based on permissions control and graphical interfaces. For instance, when the CTA Operator transmits information to the CIS Operator, this information is simultaneously received by different rescuers who have the corresponding access rights. However, by referring to the interaction model presented in Chapter 4, the receiver of each message should be taken into consideration. In this context, when a user transmits information, s/he must be able to identify the receiver of this information. We are also aware of the limitation of our work in this context. After having created the intervention and created the different assignments in the database, one is able to connect to the intervention, select her/his context, and communicate with other actors. The selection of the context aims mainly at retrieving the corresponding template. Accordingly, with each user created we logged in and connected to the *intervention1*. Figure 7.19 shows the selection and connexion to the intervention created previously. In addition, for each of those users, we selected the corresponding context. Figure 7.20 illustrates the selection of the context created for the CTA Operator. The corresponding template is

7. EXPERIMENTATIONS

Select intervention

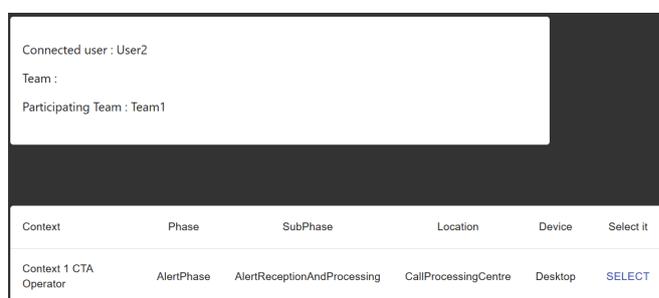
Intervention1 ▾

SUBMIT

Figure 7.19: Selection and connexion to an intervention by the CTA Operator.

then retrieved. In addition, different buttons required for creating, transmitting, and deleting the groups of information are automatically added to the groups on the basis of the group's category in order to obtain a final graphical interface. Figure 7.21 illustrates the graphical interface for the CTA Operator based on the template created and illustrated in Figure 7.16. As we can see in Figure 7.21, the groups that require the creation of one or several group instances before their fulfilment and transmission include a single button. The latter represented by the (+) button allows creating instances of the group upon requirements. Following this creation, the transmission and delete buttons are added to each created instance of the group. However, for the groups that do not require the creation of instances, the transmit and delete buttons are added directly to the group of information.

Based on the scenario described in 7.4.1, the intervention starts with receiving a call in the CTA by the CTA Operator. The latter will then select her/his context created previously and get the corresponding template. Afterwards, he will gather first information about the incident and fulfils those information in the system. Hence, four groups of information are fulfilled based on the call information. Those groups are: *Intervention Site General Information*, *Incident Information*,



Connected user : User2
Team :
Participating Team : Team1

Context	Phase	SubPhase	Location	Device	Select it
Context 1 CTA Operator	AlertPhase	AlertReceptionAndProcessing	CallProcessingCentre	Desktop	SELECT

Figure 7.20: Selection of the context created for the CTA Operator.

Figure 7.21: Graphical interface for the CTA Operator in the selected context.

Specific Dangers, and *Victims General Information* as shown in Figure 7.22. As we can see in Figure 7.22, the CTA operator fulfils different groups of information. Regarding the group *Victims General Information*, the operator creates two instances of this group for each victim respectively. After having fulfilled the call information in the system, and consulted cartography information, the CTA

Figure 7.22: Fulfilment of call information in the system by the CTA Operator.

7. EXPERIMENTATIONS

Operator selects the centre and material to engage as well as the actor to involve. Hence, based on the scenario, the CTA Operator decides to engage two vehicles as well as four actors. Following this decision, the CTA Operator will engage those resources through a departure ticket. Accordingly, this operator fulfils the corresponding groups of information that were not already fulfilled during the first task. Regarding the *Intervention Site Accessibility information*, this group is fulfilled based on the locations of the engaged centre and the intervention site respectively. Each group is then transmitted to the CIS Operator of the selected centre as illustrated in Figure 7.23. We notice that the CTA Operator is capable to read and fulfils different values in those groups since he has write and read access on those groups. In addition, he belongs to a team that participates in the intervention. Hence, different permissions control requirements are fulfilled in this context. Figure 7.23 represents the fulfilment and transmission of different groups that compose the departure ticket by the CTA Operator. Following the transmission of departure ticket information, a new phase called Involvement of required resources starts with the sub-phase: *Reception of departure ticket in CIS*. As mentioned in 7.3.2, the latter sub-phase has a single participating role: the CIS Operator. Hence, the CIS Operator will select her/his context created for this sub-phase. Following this selection, this Operator will get the adequate graphical interface based on the template designed and illustrated in Figure 7.17.

The screenshot displays a web application interface for managing emergency response information. At the top, there is a navigation menu with buttons for 'MENU', 'CONTEXT', 'CREATE CONTEXT', 'COMPONENTS', and 'LOGOUT'. A green notification bar at the top center shows a checkmark and the text 'Transmit went successful'. The main interface is divided into several panels:

- Intervention Site General Information:** Includes fields for 'SiteFunction' (Transportation Facility), 'SiteType' (Public Place checked), and buttons for 'TRANSMIT' and 'DELETE'.
- Intervention Site Accessibility Information:** Includes fields for 'RoadToTake' (Rocade Troyes), 'Address' (0206 Troyes France), 'Distance' (3 km), and 'TimeToArrive' (10 minutes). Buttons for 'TRANSMIT' and 'DELETE' are present.
- Specific Dangers:** Includes a 'Danger' field (Fuel Leakage) and a 'Localisation' field (Right side of the road). Buttons for 'TRANSMIT' and 'DELETE' are present.
- Incident Information:** Includes fields for 'Incident' (Transport Accident), 'Address' (0206 Troyes France), and 'Time' (October 3rd 11:58 p.m.). Buttons for 'TRANSMIT' and 'DELETE' are present.
- Material To Engage:** Includes a 'Material' field (Rescue And Assistance Vehicle - Road R) and an 'ID' field (FF654123). Buttons for 'TRANSMIT' and 'DELETE' are present.
- Victims General Information:** A large panel with multiple checkboxes for 'Absolute Emergency', 'Victim Status' (Good checked), 'Sex' (Male checked), 'Age' (Child checked), 'AgeRange' (Mature checked), and 'Gravity' (Slightly Injured). Buttons for 'TRANSMIT' and 'DELETE' are present.
- Actor To Involve:** Includes a dropdown for 'OrganizationMemberRole' (Driver), checkboxes for 'Firefighters', 'Medical Services', 'Health Care Facility Unit', and 'Police'. It also has fields for 'Name' (Jean), 'AgentFunction' (Volunteer), and 'Skills' (Civil Safety). Buttons for 'TRANSMIT' and 'DELETE' are present.

Figure 7.23: Fulfilment and transmission of groups that compose the departure ticket by the CTA Operator.

7.4 Scenario of incident

In addition, different information values of the groups transmitted by the CTA Operator will be received and visualised by the CIS Operator since he has Write and Read access on those groups. Figure 7.24 represents the reception of different groups that compose the departure ticket by the CIS Operator. After having received the departure ticket information, a new sub-phase begins. In the latter, the CIS Operator transmits a confirmation of this reception as illustrated in Figure 4.9. Afterwards, this operator moves to the third sub-phase of the phase entitled *Involvement of required resources*. Hence, he selects a new context created on the basis of this sub-phase. Once the context is selected, the corresponding template illustrated in Figure 7.18 will be retrieved and displayed to this Operator. In addition, different information values of distinct groups transmitted by the CTA Operator will be displayed in the right components. Accordingly, the CIS Operator transmits those different groups to the CRO as well as other rescuers involved in the intervention as shown in Figure 7.25. During the same sub-phase, different rescuers represented by the CRO, sappers, and drivers are involved. Their unique task in this sub-phase is receiving the departure ticket information transmitted by the CIS. Hence, in this example, the CRO selects her/his context created for this sub-phase. Accordingly, the template created for this context and illustrated in Figure 7.13 is retrieved. Furthermore, different groups of information transmitted by CIS Operator are retrieved and visualised

The screenshot displays a dashboard with several information panels for an incident. The panels include:

- Intervention Site General Information:** SiteFunction: Transportation Facility, SiteType: Public Place (checked).
- Material To Engage:** Material: Rescue And Assistance Vehicle - Road Re, ID: FF654123, FF987654.
- Incident Information:** Incident: Transport Accident, Address: D206 Troyes France, Date/Time: October 3rd 11:58 p.m.
- Victims General Information:** Absolute Emergency (checked), Relative Emergency, Good (checked), Relative Emergency, Localisation: Back car "101223456", Red car "9876543", Name: Maxime DUMOULIERI, Sex: Female (checked), Age: 8, Child (checked), Mature (checked), Gravity: Slightly Injured.
- Intervention Site Accessibility Information:** RoadToTake: Rocade Troyes, Address: D206 Troyes France, Distance: 2 km, TimeToArrive: 10 minutes.
- Specific Dangers:** Danger: Fuel Leakage, Localisation: Right side of the road.
- Actor To Involve:** Firefighters (checked), Medical Services, Health Care Facility Unit, Police, Volunteer (checked), Civil Safety: Vo567, Pro583.

Figure 7.24: Reception of groups that compose the departure ticket by the CIS Operator.

7. EXPERIMENTATIONS

by the CRO as illustrated in Figure 7.26. Different groups of information illustrated in Figure 7.26 are retrieved and visualised by the CRO since the latter has the corresponding access rights. For instance, the CRO has read access on *Intervention Site Accessibility Information*, *Intervention Site General Information*,

The screenshot displays the 'Actor To Involve' interface with several panels:

- Actor To Involve:** A list of roles with checkboxes for selection. Roles include Firefighters, Medical Services, Health Care, Facility Unit, Police, Professional, and Volunteer. Skills like Civil Safety and Vo543 are also listed.
- Intervention Site Accessibility Information:** Fields for Road/Route (Rocade Troyes), Address (D206 Troyes France), Distance (12 km), and Time to Arrive (10 minutes).
- Material To Engage:** A table listing materials such as 'Rescue And Assistance Vehicle' and 'Road Rescue Vehicle' with their respective IDs and transmission/delete buttons.
- Victims General Information:** A form for victim details including status (Absolute/Relative Emergency, Dead/Good), localisation (Black car 'RT123456', Red car 'AB45678'), name (Alex DUPONT, Marine DUMOULIN), sex (Male/Female), age (8/46), age range (Child/Mature/Old/Young), and gravity (Slightly Injured/Severe).
- Intervention Site General Information:** Fields for Site Function (Transportation Facility) and Site Type (Private/Public Place).
- Specific Dangers:** Fields for Danger (Fuel Leakage) and Localisation (Right side of the road).
- Incident Information:** Fields for Incident (Transport Accident), Address (D206 Troyes France), and Time (October 3rd 11:58 p.m.).

Figure 7.25: Transmission of different groups that compose the departure ticket to the involved actors.

The screenshot shows the CRO interface receiving information from the Actor To Involve interface:

- Intervention Site General Information:** Shows Site Function (Transportation Facility) and Site Type (Public Place).
- Intervention Site Accessibility Information:** Shows Road/Route (Rocade Troyes), Address (D206 Troyes France), Distance (12 km), and Time to Arrive (10 minutes).
- Specific Dangers:** Shows Danger (Fuel Leakage) and Localisation (Right side of the road).
- Material To Engage:** Shows a table with materials like 'Rescue And Assistance Vehicle' and 'Road Rescue Vehicle'.
- Victims General Information:** Shows victim status (Absolute Emergency, Good), localisation (Black car 'RT123456', Red car 'AB45678'), name (Alex DUPONT, Marine DUMOULIN), sex (Female), age (8/46), age range (Mature), and gravity (Slightly Injured/Severe).

Figure 7.26: Reception of groups that compose the departure ticket by the CRO.

Actor to involve, and *Material to engage*. Moreover, the CRO has write and read access on the groups *Specific dangers*, *Victims general information*, and *Incident information*. Moreover, the CRO can update the four latter groups upon requirements. However, none of those groups can be deleted by the CRO since they were created by the CTA Operator. Figure 7.27 the response illustrated to the CRO in case of deleting the group entitled *Incident Information*. As we can see in Figure 7.27, when the CRO tries to delete the group Incident Information, a notification message stating that he does not have the access rights is displayed. After having received the departure ticket information, the CRO and other rescuers will then prepare for the departure and move towards the intervention site to handle the operation and evacuate victims. The main important aspect that we can notice here is that different information values can be transmitted and received by different actors even if they are in different contexts. In addition, it is possible to design two different templates for two contexts by the same user even if those contexts have the same contextual information.

In this section, we showed an example of using the platform developed for communicating in rescue operations. To this end, we described a scenario of a road incident. Afterwards, we showed how different users can connect to intervention and select their context in the latter. In addition, we proved how the relevant templates are retrieved based on the selected context. Furthermore, we illustrated through an example of how different buttons required for transmitting, creating, and deleting groups of information are added to those groups in the templates. Eventually, we showed an example of transmission, reception, and deletion of information in a rescue intervention using the developed platform. We notice that, in its current version, the developed platform does not include an interface for

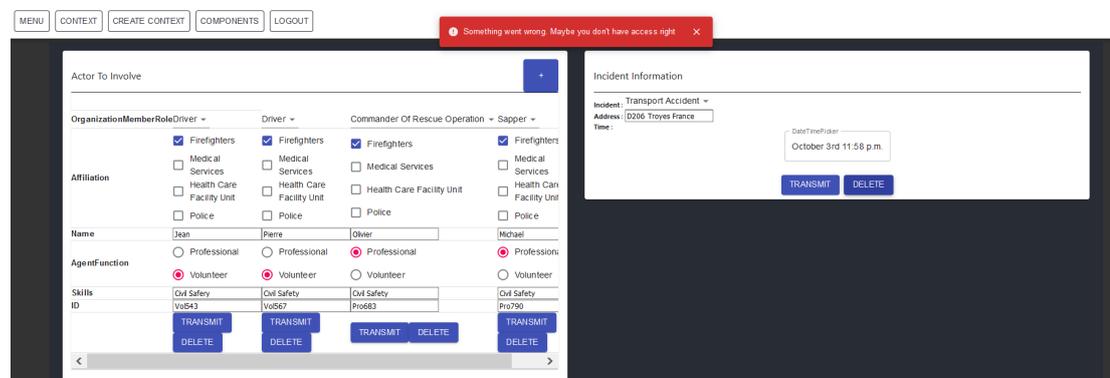


Figure 7.27: Deletion of the group *Incident Information* by the CRO.

7. EXPERIMENTATIONS

creating interventions, assigning different teams to interventions, and assigning users with those teams. Hence, in order to describe the communication scenario, we created those assignments manually in the database.

7.5 Conclusions

In this thesis, we proposed an approach for designing a communication system that supports situation awareness and communications in rescue operations. To show the relevance of our solutions, we have developed the conceived platform on the basis of the specifications described in Chapter 6. In this chapter, we presented an overview of different technologies used in the platform. Moreover, distinct functionalities included in the platform were presented. Furthermore, different mechanisms and functions integrated into the platform were discussed. Eventually, we presented a detailed use-case of the proposed platform. Hence, we designed different interfaces for multiple users by selecting specific contexts for each user based on the interaction model presented in Chapter 4. In addition, we configured several specifications for multiple groups of information. We then described a communication scenario using the platform in the case of a road accident based on the interaction model presented in Chapter 4.

Based on the design and communication example presented and the results obtained in this chapter, we believe that the methodology proposed in this thesis serves for designing and implementing a customised communication platform for rescue operations that guarantees confidential access to information. This platform meets different criteria that an efficient, usable and confidential awareness and communication-support system has to fulfil in order to be useful in rescue operations. Unfortunately, in its current version, the developed platform has several limitations. First, this platform does not include an interface for creating an intervention, assigning different teams to an intervention, and assigning users with those teams. Second, in this platform, it's not possible to select the receiver of each information. Every transmitted information is automatically received by all the actors that have the rights to access this information. However, the receiver of each message should be taken into consideration. Third, related to the specifications related to information, only the required functions related to the informational component and the field type are considered among different properties. However, other properties represented by the data type of each information, the degree of its criticality, the orientation, and the category must

be considered. Fourth, regarding the informational components, it is essential to make the difference between input and output interface components. In its current version, only the informational components that can be used for input and output at the same time are considered. Fifth, related to media components, end-users are able to integrate output media components in their interfaces. However, the integration of input media components and different functions related to media transmission and reception are not considered in the platform. Sixth, in the current version of the platform, each user must select her/his context in the intervention in order to retrieve the corresponding interface. When a user must change her/his context, the user must change it manually. However, in real practices, users do not have the time to change their context during an intervention. The switch from a user's context to another context must be managed automatically. Seventh, some groups of information have special cases. Those groups are generally independent from the interventions. Hence, they differ from the other groups in terms of design and consulting. The special case of those groups is not considered in this platform. Eighth, different functionalities and algorithms required for the management and allocation of resources were not studied not implemented in the platform. Eventually, since the proposed platform is oriented for rescue actors, it should be tested by its end-users in a real scenario to evaluate it. In this work, we did not have the opportunity to test the platform by its end-users. This should be improved for a real system that can be used by rescue actors.

7. EXPERIMENTATIONS

Chapter 8

Conclusions

Contents

8.1	General Conclusion	250
8.2	Limitations and Perspectives	255

8. CONCLUSIONS

8.1 General Conclusion

Cognitive scientists have long believed that perception and action are two servants of the mind, existing in opposite wings of the mental mansion. According to this point of view, perception and action are independent mechanisms where perception delivers messages from the outside world to keep the mind informed, and action performs what the mind commands. More recent studies have boosted the idea of the existence of solid links between perception, action, and decision-making. According to [De Oliveira *et al.*, 2009], those links are bidirectional and constrained. By bidirectional, it is meant that each of those mechanisms affects the other mechanisms. Of course, one's perception of a situation highly affects this one's actions. Those actions may also influence and orientate one's perception. On the other hand, constrained means that those links are affected by the characteristics of the action and the environment. The interconnections between perception, decision-making, and action are crucial for many human interactions. Several researchers assume a direct way of humans interaction based on the strong interconnection between action and perception [Knoblich & Sebanz, 2006]. Indeed, in collaborative environments that imply the involvement and cooperation between different actors, perceiving others' actions and situations constitutes a basic element for making appropriate decisions, executing relevant actions, and enhancing interactions. Several studies have been proposed in the literature to support decision-making. Most of those studies were mainly based on proposing decision-support systems. Unfortunately, in multiple collaborative environments, actors still lack the backing to perceive others' situations and actions. The research presented in this thesis aimed at supporting situations' perception in order to enhance decision-making and thus actors' actions and performance in collaborative environments. In this context, the main objective of this work is to ensure that collaborating actors a common perception of situations even if they are geographically dispersed. This perception must be as close as possible to reality. In order to respond to this problematic, we propose to support awareness in those environments. There exist several types and categories of awareness. In this thesis, we chose to support situation awareness since it is a critical element for decision-making in critical and collaborative environments. Hence, the first general research question that one can ask in this context is: **How to guarantee situational awareness amongst participating actors in collaborative environments?**

Based on the definition of situation awareness, a key first step toward achieving it and reaching its highest levels consists in ensuring a common perception of situations amongst collaborating actors. Therefore, we propose to ensure a common perception and understanding of situations between collaborating actors in collaborative environments in order to enhance situation awareness amongst those actors. A second research question can be formulated in this context as follows:

How to ensure a common perception of situations between actors?

One of the most effective solutions toward ensuring a common perception of situations between actors relies on guaranteeing efficient information exchange and communication between those actors. This solution leads to a third question:

How to guarantee effective communications in collaborative environments?

The main solution to this question consists in proposing a communication and information exchange system that guarantees the communication of the right actionable information, to the right person, at the right time. The system should be adaptable to the users' contexts. Moreover, it must ensure a common understanding of the messages and concepts between different actor's to ensure the common perception of situations. Semantic representation techniques and ontologies can be very helpful in order firstly to represent the main situation's entities, to guide situation's perception sharing. Accordingly, the solution to this question consists in enhancing interactions and information exchange through an ontology-based communication-support system. It is therefore required to define an ontology that captures the knowledge related to communication in the target domain. Moreover, it is necessary to consider the real practices and interactions of those users in the design of the system in order to propose an adaptable system according to the users' contexts. Therefore, it is of great importance to study, analyse, and model those interactions and practices before the design and implementation phase. This leads to identifying the requirements, criteria, and real needs of actors on the basis of real practices and thus to propose a usable communication system. The communication system must also gain the acceptance and acceptability of its end-users. Users' acceptability is one of the basic prerequisites of any user support tool and assistive technology. A fourth question that can be formulated here is: **How to guarantee the acceptability of the proposed system by its end-users?**

8. CONCLUSIONS

To ensure the users' acceptability of the proposed system, this latter must support the central process and practices efficiently. The system must also be flexible to any modification upon requirements. Involving users in the design of the system is the best way to increase the acceptability and usability of the systems. We thus propose to allow the end-users of the system to define its interfaces and specifications by themselves based on their roles, tasks, and contexts. This will also help to enhance situation awareness amongst those actors. Moreover, using ontologies for the system's design guarantees that the system meets the flexibility requirements. Hence, knowledge related to the design of systems and interfaces must be integrated into the ontology. Therefore, the third solution consists in proposing an approach through which final users can design the system in a customised way based on a semantic representation of knowledge. Accordingly, we proposed an approach for designing the system specifications and interfaces in a dynamic and customised way. Eventually, for some collaborative environments that imply the exchange and communication of personal and sensitive information, it is required to guarantee the confidentiality of information. Hence, a fifth question can be formulated as follows: **How to guarantee confidential access to information in the system?**

In order to guarantee the privacy of information, adequate mechanisms and techniques must be integrated into the communication system. In this manner, it is necessary to adapt the adequate confidentiality policies and mechanisms to the users' needs. Hence, those mechanisms shall be chosen on the basis of the practices and interactions. Accordingly, the solution to this question consists in choosing relevant confidentiality policies and mechanisms in a way that meets the stakeholders' needs. In this context, multiple mechanisms must be integrated such as data encryption, authentication, access control, as well as other mechanisms related to the security of communication infrastructure. Moreover, the knowledge related to those mechanisms must also be integrated into the ontology in order to preserve the flexibility of the system. In this work, we only focused on a single aspect that is access control and rights management in the communication system since other mechanisms like data encryption can be ensured with standard tools.

In order to prove the relevance of those assumptions, we took in this thesis the case of French rescue operations as the target collaborative environment. In this context, we proposed an approach for designing a customised awareness and

communication-support system oriented for rescue actors that guarantees the confidentiality of information. The motivation behind choosing the rescue domain is justified for many reasons. First, the domain of rescue requires high performance of rescue actors. It implies the collaboration between a large number of actors that come from different backgrounds with specific missions and goals. Hence, it is essential to ensure a shared perception of situations and a high level of awareness amongst stakeholders. Second, rescue actors are mostly geographically dispersed. They have to make decisions and act based on the situation perceived by other actors. Accordingly, it is essential to enhance the perception of situations in order to ensure the execution of relevant actions. Third, each actor has a specific role with corresponding tasks to achieve and personal preferences. Therefore, it is required that the proposed system meets the needs and preferences of each actor. Fourth, in rescue operations, a large amount of medical information is exchanged between rescue actors. It is then essential to reinforce the confidentiality of information in the proposed system. Fifth, despite the large number of communication systems oriented for rescue operations, communication during those operations is still limited to oral communication using radio devices. We notice that, in this thesis, we focus our study on daily rescue operations that imply the participation of firefighters and medical services. However, the work presented does not cover large-scale and disaster response operations that imply the activation of specific plans such as ORSEC and the implication of additional actors with particular roles. In most of the countries, the rescue actors still lack baking in information exchange and communication. The proposed approach consists of a five-step methodology.

The first step approach consists in examining and modelling interactions based on real practices. The importance of this step is to identify the information required by each person based on her/his role, context, and tasks to achieve. Accordingly, we analysed different interactions in daily rescue operations based on a deep study of documents, reports, and legislation related to the domain. We identified required elements and parameters to be taken into account when modelling interactions in complex contexts such as rescue operations. Those elements are *Actors*, their *Roles* and their *Positions* in the organisational levels of operations, *Information*, *Communication instrument*, *Tasks*, *Time*, and *Location*. We then proposed an interaction model that shows interactions between different actors in French rescue operations. This model allows efficient extraction of dependencies between Actor and Role, Task, Information, Communication device, Operation

8. CONCLUSIONS

phase, Location, and Time. Moreover, this model serves as a basis to define the communication system specifications based on communication protocols defined in rescue operations and thus, to support the representation of situations (Cf. Chapter 4).

The second step relies on constructing an application ontology that represents the knowledge required for designing a communication system oriented for rescue actors that guarantees confidential access to information. Hence we developed an application ontology called ResOnt for this aim. This ontology consists of three modules. The first module, called ResOnt Rescue and Communication, is oriented for representing knowledge related to communications in rescue operations. It serves for ensuring a shared interpretation of information between different stakeholders as well as representing and formalising different procedures and flow of information. The second module, entitled ResOnt Design, incorporates knowledge required for the dynamic design and configuration of the system and interfaces. Whereas, the third module, ResOnt Access Control, is specific for representing static knowledge required for guaranteeing access control management in the system. To develop this ontology we adopted METHONTOLOGY as the methodology for construction and reused several existing ontologies related to different aspects. In addition, we instantiated this ontology mainly based on the interaction model. ResOnt ontology answers the totality of proposed Competency Questions (Cf. Chapter 5).

The third step consists in developing an ontology-based platform for design and communication. This platform will allow the end-users to define the system's specifications and design its interfaces in a customised way. Accordingly, we presented a design and communication platform based on the interaction model presented in Chapter 4 and ResOnt ontology presented in Chapter 5. Different functionalities and requirements needed in the platform were described in detail. In addition, the general architecture, as well as detailed descriptions of data flow were provided. In this platform, it is possible to configure the specifications related to information in a dynamic way. Moreover, each user can create different contexts and configure their elements based on her/his associated role. Furthermore, a user can check different information elements required in a context. In addition, it is possible to create and design personalised templates related to the users' identities and the contexts created. In this context, the user can integrate the required media components. This user can also position different components on the template in a way that meets her/his preferences. Following this

design, each user can connect to a created intervention, select her/his context, and communicate with other actors (Cf. Chapter 6).

The fourth step relies on integrating confidentiality mechanisms in the system. As mentioned above, in this thesis, we focused on the access control mechanism. In this context, we proposed an access control and rights management policy to guarantee the confidential access to information in the platform. To this end, we adapted and modified the TT-RBAC model and proposed a new access control model. The aforementioned policy is based on two main activities: Rights management, and Permissions control. Hence, we described the different steps and aspects related to rights management. Those rights were determined on the basis of static knowledge in the ontology. In addition, we proposed different algorithms to control permissions in the platform based on static knowledge and dynamic information (Cf. Chapter 6).

The fifth step consists in designing the system's specifications and interfaces by its end-users in a customised through the proposed platform. Hence, we implemented a first prototype of the platform. In addition, we developed and integrated different required functions and mechanisms into the developed platform. Moreover, we realised several experiments related to design and communication using the developed platform. In this context, we showed the possibility of designing customised interfaces in this platform in a flexible and dynamic way. Furthermore, we presented a communication scenario using the platform in case of a fictitious road accident (Cf. Chapter 7).

8.2 Limitations and Perspectives

The research work presented in this thesis has different limitations. As part of short and mid-term perspectives, we would like to investigate the following aspects concerning improvements of our proposed solutions:

- *Extending the proposed interaction model:* To analyse and model different interactions, we adopted an approach based on a scenario description. In this context, we described a scenario of a small-scale rescue operation in France following an incident that affects several victims. In this scenario, only two services were considered: Firefighters, and Medical Services. However, in real scenarios, other services may be involved such as the Police. Moreover, the application of this model is limited to small-scale daily rescue

8. CONCLUSIONS

operations. However, it should be extended to cover large-scale operations also. Accordingly, this model should be generalised to cover different possible scenarios. In this context, different types of incidents and services must be considered.

- *Validating the proposed interaction model:* For reasons related to time and confidentiality, we were unable to access the field in order to analyse the real practices of the rescue actors. Moreover, although this model was based on a deep study of domain-related documentation, we were not able to meet domain experts to validate it. Therefore, we propose to validate this model with a real case study in order to evaluate it by domain experts.
- *Completing ResOnt Ontology:* Several concepts related to the design of systems and interfaces were not defined in ResOnt. For instance, input media components and other elements were not considered in this work. Moreover, other aspects related to communications such as infrastructures and networks were not considered in ResOnt. In addition, related to information confidentiality, since this work focus on access control mechanisms, the definition of concepts in ResOnt was limited to the concepts in relation to this mechanism. In this context, we propose to complete ResOnt ontology in order to cover different aspects related to the design, communication, and information confidentiality.
- *Evaluating ResOnt Ontology by domain experts:* There exist several approaches for ontology evaluation. In this thesis, we adopted the application-based approach to evaluate ResOnt ontology. However, the user-based approach allows a better and more complete evaluation compared to other approaches. Unfortunately, during this thesis, we were not able to meet a domain expert after the ontology development to evaluate it. Hence, we could not adopt this approach. Hence, an evaluation of ResOnt ontology by domain-experts is proposed as future work. Following this evaluation, we will enrich this ontology upon requirements and suggestions.
- *Implementing a complete platform that includes different functionalities:* In this thesis, the implementation work was limited to developing a local platform that allows the design of interfaces as well as the local exchange of information. Unfortunately, due to time limitations, several important aspects related to communication such as the orientation of messages were not considered in this work. Moreover, different functionalities required for

the management and allocation of resources were not studied nor included in the developed platform. As future work, this platform must be extended into a complete system that takes includes different required functionalities and mechanisms. In addition, several improvements on the developed functionalities in the current version must be performed. Besides, a study of different communication architectures and networks must be carried to adopt the most relevant one.

- *Testing and evaluating the developed platform by end-users:* In this thesis, in order to test the developed platform, we performed two experiments to evaluate the platform's functionalities in terms of design and communication. To this end, we described a fictitious design and communication scenario in case of road accident. However, this platform must be tested and evaluated by its end-users. Accordingly, we propose to provide this platform to the involved services in rescue operations in order to test it in real scenarios. Several modifications and enrichments can be then performed on the platform upon the needs, requirements, suggestions, and feedbacks of the end-users.

As for long-term perspectives, we look forward to:

- *Making ResOnt ontology publicly accessible:* Since ResOnt ontology is not evaluated by the domain experts, we did not make it publicly accessible. Hence, following its evaluation, we look forward to submitting it and publishing it in an ontology catalogue.
- *Extending the application of the proposed approach to other environments:* In this thesis, the application of the proposed approach was limited to the domain of rescue operations. We propose to study the application of this approach in other collaborative environments to validate its relevance.

8. CONCLUSIONS

Appendix A

Résumé de la thèse

Contents

A.1	Introduction	261
A.1.1	Questions de recherche, solutions, et méthodologie	262
A.1.2	Contributions	266
A.2	Communication d'information	267
A.2.1	Modèles de communication pour le secours à personne	267
A.2.2	Systèmes de support à la communication	267
A.3	Ontologies et représentation des connaissances	268
A.3.1	Définitions	269
A.3.2	Méthodologies de construction des ontologies	269
A.3.3	Ontologies pour le secours et la gestion des urgences	271
A.3.4	Approches et ontologies pour la conception de systèmes et d'interfaces	272
A.3.5	Approches et ontologies pour le contrôle d'accès	272
A.4	Modélisation des interactions	274
A.4.1	Secours à personne en France	274
A.4.2	Modèle organisationnel	275
A.4.3	Modélisation des interactions et des communications	276
A.5	Ontologie ResOnt	279
A.5.1	Méthodologie de développement	280
A.5.2	Description de l'ontologie ResOnt	284
A.6	Plateforme de support à l'awareness	288

A. RÉSUMÉ DE LA THÈSE

A.6.1	Principes de base	288
A.6.2	Fonctionnalités et architecture	290
A.6.3	Identification du contexte	291
A.6.4	Configuration et conception dynamiques et person- nalisées	293
A.6.5	Communication et contrôle d'accès	294
A.7	Expérimentations	296
A.8	Conclusions et perspectives	298
A.8.1	Conclusion générale	298
A.8.2	Perspectives	299

A.1 Introduction

Le problème abordé dans nos travaux est la prise de conscience mutuelle dans un domaine complexe et dynamique qui est le domaine du secours. Nous abordons particulièrement le partage efficace de l'information comme première étape pour aider à cette prise de conscience. L'amélioration de la communication et du partage d'informations dans les opérations de secours a fait l'objet de nombreuses études au cours des dernières décennies. De nombreuses solutions ont été développées pour tenter de résoudre des problèmes importants qui conduisent à une prise de décision inefficace comme le manque de conscience de la situation et l'inefficacité dans le partage d'informations. Dans ce contexte, plusieurs systèmes ont été développés pour soutenir l'échange d'informations et la communication. Pourtant, dans la plupart des pays, la communication lors des opérations de secours est encore limitée à la communication orale à l'aide des appareils radio [Mallek *et al.*, 2016]. En effet, la plupart des systèmes existants ne sont pas pleinement acceptés par les acteurs puisqu'ils sont limités à certaines fonctionnalités ou sont développés sans examiner les activités réelles des acteurs. Plusieurs études font état d'une faible adoption des systèmes de communication dans les opérations de secours ainsi que d'une position négative des acteurs envers ces systèmes [Elmasllari, 2019]. Les besoins réels des parties prenantes, tout simplement, ne sont pas pris en compte par les systèmes proposés. En observant ce problème à travers un point focal de conception, nous remarquons que ces problèmes proviennent généralement de l'utilisation de techniques de conception non pertinentes ainsi que d'approches inadéquates pour collecter les préférences des utilisateurs et aider à une prise de conscience mutuelle des situations. Ainsi, un besoin vital de proposer un système de communication qui soutient les communications, réponde aux besoins des parties prenantes et gagne leur acceptation et acceptabilité est souligné. Cependant, la conception de systèmes pour les utilisateurs qui travaillent dans des domaines complexes tels que les opérations de secours reste un défi. Cela est dû à de nombreuses raisons. Premièrement, une bonne approche de conception de système nécessite la collecte de l'ensemble des exigences et préférences des utilisateurs de manière à proposer un système pertinent et facile à utiliser. Dans le domaine du secours où plusieurs acteurs issus de plusieurs organisations différentes participent à une même opération, il est difficile de répondre à cette exigence car les utilisateurs appartiennent à des différentes organisations avec des rôles distincts. Cela impose de proposer des spécifications et des interfaces à l'utilisateur en fonction de son rôle. Le deuxième

A. RÉSUMÉ DE LA THÈSE

problème important est la diversité des contextes et des tâches à accomplir. Par exemple, les acteurs participants se trouvent dans différents endroits avec des tâches distinctes à accomplir. Les participants sont censés recevoir, consulter ou transmettre des informations en fonction de la tâche à traiter. Cela entraîne une hétérogénéité des informations à échanger en fonction de chaque contexte et tâche, ce qui compliquera sûrement la phase de conception. De plus, les informations échangées pendant le secours peuvent prendre plusieurs formes telles que du texte, de l'audio, de la vidéo, du signal ou des graphiques. Cette diversité nécessite de concevoir le système de manière à prendre en compte ces différentes formes. Enfin, une grande quantité d'informations échangées est de nature sensible comme les informations personnelles liées à l'état de santé des victimes. Par conséquent, garantir la confidentialité de ces informations est obligatoire. Ainsi, il est très important de prendre en compte la confidentialité des informations dans la conception du système. Toutes les raisons et difficultés mentionnées font de la conception de systèmes de communication pour les acteurs du secours une tâche très difficile.

A.1.1 Questions de recherche, solutions, et méthodologie

Le projet de recherche présenté dans cette thèse s'inscrit dans la définition d'un système flexible qui améliore le partage d'informations, le premier support à la conscience dans un domaine émergent, collaboratif, complexe et dynamique, qui est le domaine du secours. Ce système est conçu de manière à garantir une conscience mutuelle entre les différentes parties prenantes. De plus, il est essentiel que le système garantisse des communications efficaces et un accès confidentiel à l'information. Enfin, il est très important de concevoir le système de manière à gagner l'acceptabilité des parties prenantes. Par conséquent, trois questions de recherche et trois solutions correspondantes ont été formulées :

Q.1 : Comment garantir une conscience mutuelle des situations entre les différents acteurs participant aux opérations de secours ?

Sur la base de la définition de la conscience, une première étape clé pour y parvenir consiste à assurer une perception et une représentation communes des situations entre les différents acteurs. Cela nécessite d'assurer un échange d'information et une communication efficaces entre ces acteurs. De plus, la cohérence de la perception des situations nécessite la définition des principaux concepts qui peuvent

représenter les activités de différents acteurs. Par conséquent, il est essentiel que le système proposé aide à représenter une perception commune des situations et des concepts entre les acteurs. Les techniques de représentation sémantique [Sowa, 1999; Studer *et al.*, 1998] et les ontologies [Gruber *et al.*, 1993] peuvent être très utiles pour représenter les entités principales de la situation et guider le partage de la perception de la situation [Nunavath *et al.*, 2013]. Par conséquent, la première solution consiste à améliorer les interactions et l'échange d'informations à travers un système d'aide à la communication basé sur des techniques de représentation sémantique et des ontologies.

Q.2 : Comment garantir des communications efficaces et un accès confidentiel aux informations lors des opérations de secours ?

Pour être utilisé par les unités opérationnelles pour l'accompagnement de leurs tâches, il est indispensable de prendre en compte les pratiques et interactions réelles dans la conception du système d'aide à la communication. Par conséquent, il est d'une grande importance d'étudier, d'analyser et de modéliser ces interactions et pratiques [Saoutal, 2015]. Cela conduit à identifier les exigences, les critères et les besoins réels des acteurs sur la base de pratiques réelles en temps non seulement, d'actions, mais également d'espaces, de temps et d'équipements. En ce qui concerne l'aspect de confidentialité, des mécanismes et techniques adéquats doivent être intégrés dans le système de communication afin de garantir la confidentialité des informations. Ainsi, la seconde solution repose sur la prise en compte des pratiques et interactions réelles dans la phase de conception. Cette solution consiste également à choisir les politiques et mécanismes de confidentialité pertinents de manière à répondre aux besoins des parties prenantes.

Q.3 : Comment garantir l'acceptabilité du système proposé par ses utilisateurs finaux ?

L'acceptabilité des utilisateurs est l'une des conditions préalables de base de toute technologie d'assistance [Wilkinson & De Angeli, 2014]. Par conséquent, l'un des défis considérables est celui de développer une technologie qui soit acceptable et utilisable par des utilisateurs finaux ayant différents arrangements de besoins, d'exigences et de capacités. Pour garantir l'acceptabilité par les utilisateurs du système proposé, il est essentiel que ce dernier soutienne le processus central et pratiques efficacement. L'acceptabilité des utilisateurs peut être étudiée à travers différentes approches. L'une de ces approches est basée sur la conception et l'ergonomie du système [Alexandre *et al.*, 2018]. De même, il existe plusieurs approches et méthodes de conception de systèmes. Impliquer les utilisateurs dans

A. RÉSUMÉ DE LA THÈSE

la conception du système est le meilleur moyen d'augmenter l'acceptabilité et la facilité d'utilisation des systèmes [Wilkinson & De Angeli, 2014]. Nous proposons ainsi de permettre aux utilisateurs finaux du système de définir eux-mêmes ses interfaces et ses spécifications en fonction de leurs rôles, tâches et contextes. Par conséquent, la troisième solution consiste à proposer une nouvelle approche par laquelle les utilisateurs finaux peuvent concevoir le système de manière personnalisée à partir d'une représentation sémantique des connaissances.

Sur la base des trois solutions proposées, nous proposons de concevoir et de mettre en œuvre un système de communication visant à simplifier le partage d'informations basé sur des techniques de représentation sémantique et une personnalisation des usages. Ce système est appelé MODES, qui signifie système d'échange de données médicales et opérationnelles. Pour être utilisé et accepté par les unités opérationnelles, il est essentiel de concevoir un tel système de manière à répondre à leurs besoins pratiques. De plus, afin de garantir la confidentialité des informations, il est essentiel d'intégrer les mécanismes appropriés dans le système proposé de manière à répondre aux besoins des parties prenantes. Dans ce contexte, de multiples mécanismes peuvent être intégrés tels que le chiffrement des données, l'authentification, le contrôle d'accès, ainsi que d'autres mécanismes liés à la sécurité des infrastructures de communication. Cependant, dans ce travail, nous nous concentrons uniquement sur un seul aspect qui est le contrôle d'accès et la gestion des droits dans le système de communication puisque d'autres mécanismes comme le chiffrement des données peuvent être assurés avec des outils standards. Nous proposons dans cette thèse une approche pour identifier les spécifications du système et concevoir ses interfaces par ses utilisateurs finaux. L'approche proposée comprend l'intégration d'une politique de contrôle d'accès et de gestion des droits pour garantir l'accès confidentiel aux informations dans le système à développer. Cette approche consiste en une méthodologie en cinq étapes comme le montre la Figure A.1.

Comme on peut le voir sur la Figure A.1, la première étape consiste à examiner et modéliser des interactions basées sur des pratiques réelles. L'importance de cette étape est d'identifier les informations requises par chaque personne en fonction de son rôle, de son contexte et des tâches à accomplir. La deuxième étape repose sur la construction d'une ontologie applicative qui représente les connaissances nécessaires à la conception d'un système de communication orienté pour les acteurs du secours qui garantit la confidentialité des informations. Cette ontologie se compose de trois modules. Le premier module est orienté

pour représenter les connaissances liées aux communications dans les opérations de secours. Il sert à assurer une interprétation commune des informations entre les différentes parties prenantes ainsi qu'à représenter et à formaliser différentes procédures et flux d'informations. Le deuxième module intègre les connaissances requises pour la conception et la configuration dynamiques du système et des interfaces. Alors que le troisième module est spécifique pour garantir la gestion du contrôle d'accès dans le système. Afin de manipuler le traitement des différentes inférences, il est important de définir des relations entre différents concepts et instances en se basant sur des interactions réelles. Par conséquent, la première et la deuxième étapes sont interdépendantes entre elles. La troisième étape consiste à développer MODES, une plate-forme pour la conception et la communication. Basée sur l'ontologie précédemment développée, cette plateforme permettra aux utilisateurs finaux du système de définir ses spécifications et de concevoir ses interfaces de manière personnalisée. L'importance d'utiliser une ontologie dans cette étape est de développer une plate-forme flexible qui permet la configuration dynamique du système. Concernant la quatrième étape, elle se situe dans l'intégration des mécanismes de confidentialité dans le système. Comme mentionné plus haut, nous nous concentrons dans cette thèse sur le mécanisme de contrôle d'accès. Dans ce contexte, nous proposons une politique de contrôle

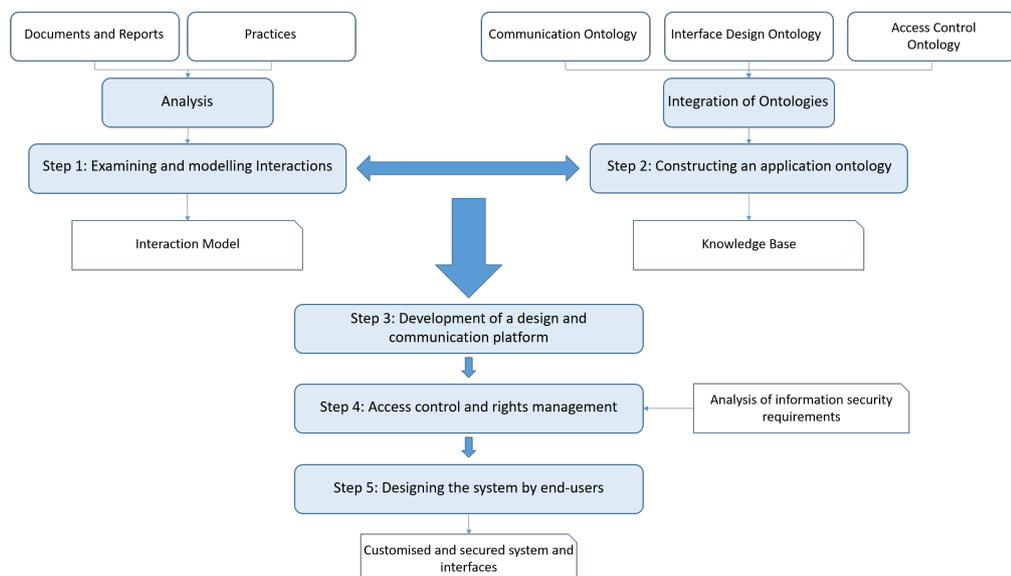


Figure A.1: Méthodologie pour concevoir un système de communication personnalisé qui garantit la confidentialité des informations.

A. RÉSUMÉ DE LA THÈSE

d'accès et de gestion des droits pour garantir l'accès confidentiel aux informations du système basé sur l'ontologie développée. Alors que la cinquième étape consiste à concevoir les spécifications et les interfaces du système par ses utilisateurs finaux de manière personnalisée via la plate-forme proposée. L'objectif de franchir ces étapes est de proposer un système utilisable et flexible qui garantit la confidentialité des informations et qui peut être accepté par les parties prenantes.

A.1.2 Contributions

Dans cette thèse nous abordons la problématique de la prise de conscience et de la communication dans les opérations de secours et proposons plusieurs contributions dans le domaine. L'apport principal est la proposition d'une démarche et d'une plateforme de conception d'un système de communication orienté vers les acteurs français du secours.

Premièrement, nous présentons une étude d'état de l'art sur des solutions de support à la communication dans les opérations de secours et la gestion des crises. De plus, les ontologies existantes en lien avec le domaine de secours, la conception, et le contrôle d'accès sont présentées.

Deuxièmement, nous modélisons les interactions entre les acteurs et identifions les besoins de modélisation.

Ensuite, nous présentons une ontologie d'application, appelée ResOnt, développée pour représenter et formaliser les connaissances nécessaires à la conception d'un système de communication orienté pour les acteurs du secours et de l'intervention d'urgence qui garantit l'accès confidentiel aux informations.

Enfin, nous présentons la plateforme MODES qui permet aux utilisateurs d'identifier et de concevoir les spécifications et les interfaces du système de manière personnalisée en utilisant le modèle d'interaction décrit et l'ontologie proposée. À l'issue de cette étape de conception, les utilisateurs finaux pourront communiquer efficacement lors des opérations de secours.

A.2 Communication d'information

Au cours des dernières années, les opérations de secours et de gestion de crise ont fusionné des technologies de l'information et de la communication, de l'intelligence artificielle, de l'informatique omniprésente, des capteurs, des robots, de l'ingénierie des systèmes et d'autres technologies. De nombreuses applications et systèmes ont été développés pour faciliter la communication et l'échange d'informations dans des domaines dynamiques et critiques tels que la gestion de crise et le secours à personne. Dans cette section, nous présentons certains travaux principaux effectués dans la littérature pour supporter et modéliser les communications dans le secours à personne et la gestion des crises.

A.2.1 Modèles de communication pour le secours à personne

La recherche sur les processus de modélisation, les communications et les interactions dans les interventions d'urgence et le secours a évolué ces derniers temps. Plusieurs modèles de processus, de communication et d'interaction sont proposés dans la littérature comme le montre le Tableau 2.2. Le tableau 2.2 présente quatre modèles sélectionnés qui ont été créés pour analyser et formaliser les connaissances liées aux processus et aux interactions dans les opérations de secours, les interventions d'urgence et la gestion des crises. Malheureusement, les dépendances entre les tâches et les informations et celles entre les rôles d'acteurs et les informations ne sont montrées dans aucun de ces modèles. Par conséquent, l'utilisation de ces modèles est limitée et nécessite une analyse plus approfondie.

A.2.2 Systèmes de support à la communication

Plusieurs systèmes ont été développés pour soutenir la conscience, l'échange d'informations et la communication dans les opérations de secours. Cependant, leur utilisation est encore limitée [Mallek *et al.*, 2016]. La raison principale de cette problématique est que la plupart de ces systèmes ne répondent pas aux critères qu'un système utilisable de communication et de sensibilisation orienté pour les acteurs du secours doit remplir. Tout système qui vise à améliorer la conscience des situations et à assurer des communications sécurisées dans les opérations de secours doit répondre à une liste de critères minimaux. Ces critères sont définis sur la base des définitions de la connaissance de la situation, de la

A. RÉSUMÉ DE LA THÈSE

documentation relative au domaine ainsi que de plusieurs études antérieures. Il s'agit notamment :

- **Prendre en compte la diversité des besoins des parties prenantes**
- **Facilité d'utilisation et personnalisation des fonctionnalités du système**
- **Flexibilité et adaptabilité**
- **Confidentialité**

Comme déjà mentionné, de multiples systèmes de communication et de sensibilisation ont été développés et orientés pour les opérations de secours et d'intervention d'urgence. Ces systèmes ont été étudiés et analysés selon les quatre critères identifiés qu'un système de communication doit remplir pour être utilisable et acceptable par différentes parties prenantes. Le tableau 2.4 montre la classification des systèmes étudiés selon les différents critères identifiés. Malheureusement, comme le montre le tableau 2.4, aucun des systèmes étudiés ne répond à tous les critères. Par conséquent, nous proposons dans cette thèse une approche pour concevoir et implémenter MODES, un système que nous souhaitons mettre en œuvre afin de soutenir les communications et la conscience de la situation et qui répondra à tous les critères identifiés. Les techniques de représentation sémantique et les ontologies sont utiles pour répondre à la majorité des critères identifiés. De plus, ces techniques sont pertinentes pour saisir, formaliser et représenter les connaissances liées au domaine d'étude. Nous présentons dans la section suivante certaines ontologies existantes en lien avec nos domaines de recherche.

A.3 Ontologies et représentation des connaissances

Avant de concevoir un système de communication orienté vers un certain domaine, il est nécessaire de capturer les connaissances liées au domaine et de les représenter à travers des techniques pertinentes. Cela garantira de développer un système qui sera accepté par ses utilisateurs finaux et qu'il s'adaptera à leurs pratiques. Pour cela, nous choisissons l'utilisation d'ontologies comme technique adéquate pour représenter les connaissances et concevoir le système. La solution proposée

repose sur trois domaines d'études distincts. Le premier domaine représente les connaissances liées aux communications dans les opérations de secours. Le second consiste à représenter les connaissances nécessaires à la conception du système et de ses interfaces. Alors que le troisième domaine se situe dans la représentation des connaissances nécessaires pour garantir le contrôle d'accès et la gestion des droits.

A.3.1 Définitions

Sowa a défini la représentation des connaissances par l'utilisation d'ontologies et de logique pour construire et formaliser des modèles dans un domaine [Sowa, 1999]. Concernant le terme Ontologie, il a été défini par Studer *et al.* [1998] comme suivant : *“une spécification formelle et explicite d'une conceptualisation partagée”*. Les ontologies sont généralement classées en cinq catégories [Falquet *et al.*, 2011]. Ces catégories dépendent du niveau de généralité de l'ontologie. La Figure 3.2 représente la classification des ontologies comme donnée dans [Falquet *et al.*, 2011]. Comme le montre la Figure 3.2, les cinq catégories sont : ontologies de haut niveau (Top-level ontologies), ontologies de niveau intermédiaire (Mid-level ontologies), ontologies de domaine (Domain ontologies), ontologies de tâches (Task ontologies), et ontologies d'application (Application ontologies). Quelque soit la catégorie de l'ontologie, il existe plusieurs raisons qui justifient l'utilisation d'une approche ontologique :

- Les ontologies permettent de spécifier des relations sémantiques entre différents concepts.
- Les ontologies permettent une compréhension commune des connaissances entre différentes entités, qu'il s'agisse d'humains ou d'agents logiciels, ce qui permet de raisonner et de traiter automatiquement les informations.
- Les ontologies sont flexibles et peuvent être réutilisées au fil du temps.
- Les ontologies peuvent être échangées entre différents acteurs, ce qui permet de résoudre les problèmes d'interopérabilité.

A.3.2 Méthodologies de construction des ontologies

Pour développer une ontologie, il est très important d'adopter une méthodologie qui gère et guide le processus de développement. En effet, la méthodologie de

A. RÉSUMÉ DE LA THÈSE

développement choisie peut considérablement affecter l'efficacité d'une ontologie. Plusieurs méthodologies pour la conception et le développement d'ontologies ont été proposées dans la littérature. Plusieurs études ont été menées pour analyser les différentes méthodologies [Corcho *et al.*, 2006; Jones *et al.*, 1998; Karray *et al.*, 2012; Mizoguchi, 2004]. Parmi ces ontologies, on peut citer METHONTOLOGY, On-to-Knowledge, Toronto Virtual Enterprise (TOVE), the Activity First Methodology (AFM), and the Unified Process for Ontology Building (UPON) Methodology. Chacune de ces méthodologies a ses exigences et son contexte d'utilisation. Cependant, ils sont généralement similaires et partagent des procédures et des étapes similaires. Les cinq étapes largement reconnues pour développer une ontologie sont la spécification, la conceptualisation, la formalisation, la mise en œuvre et l'évaluation [Pinto & Martins, 2004]. Selon [Corcho *et al.*, 2003], METHONTOLOGY et On-to-Knowledge sont les plus complètes. De plus, elles sont très utiles pour construire des ontologies à grande échelle [Mizoguchi, 2004]. Alors que Corcho *et al.* [2003] déclare que la METHONTOLOGY est la plus mature. Par conséquent, nous adopterons METHONTOLOGY afin de développer les ontologies nécessaires à notre approche. Malheureusement, dans ce travail, nous n'avons pas eu l'occasion de rencontrer des experts du domaine censés aider dans l'acquisition des connaissances et les étapes d'évaluation de l'ontologie. Par conséquent, nous avons proposé de développer l'ontologie requise en se basant sur la documentation relative au domaine ainsi que sur les ontologies existantes.

Comme cela a été mentionné dans la section [A.1.1](#), nous proposons dans cette thèse une approche ontologique pour concevoir un système de communication orienté vers les opérations de secours. Cette approche comprend l'intégration d'une politique de contrôle d'accès pour garantir l'accès confidentiel aux informations dans le système à développer. Outre les aspects de communication et d'interaction, il est essentiel d'aborder les aspects de conception et de contrôle d'accès. Dans les sections [A.3.3](#), [A.3.4](#) et [A.3.5](#), nous présentons les travaux existants liés aux ontologies pour le secours et les interventions d'urgence ainsi que les approches basées sur l'ontologie pour concevoir des systèmes et des interfaces et garantir le contrôle d'accès.

A.3.3 Ontologies pour le secours et la gestion des urgences

En lien avec notre objectif, plusieurs travaux ont été distingués dans le cadre de l'ingénierie des connaissances pour construire des systèmes à base de connaissance orientés pour la gestion des crises et des urgences. En outre, plusieurs systèmes basés sur les ontologies ont été développés pour soutenir la conscience, l'échange d'informations et la communication dans les opérations de secours et d'intervention d'urgence. À cette fin, de multiples ontologies de domaine, de tâche et d'application ont été proposées dans ces domaines. De plus, plusieurs ontologies de domaine et d'application ont été construites dans le contexte de la gestion de crise et du domaine de réponse aux catastrophes à grande échelle. Le tableau 3.1 présente un résumé des ontologies analysées qui ont été développées pour formaliser les connaissances liées à ces domaines. Dans les différentes ontologies proposées, divers aspects sont représentés comme : l'étude et l'analyse des tâches, des communications, des opérations, des organisations, des ressources, et bien d'autres aspects. Chacune d'ontologie a ses objectifs et son intérêt de recherche. Malheureusement, certaines de ces ontologies ne sont pas accessibles au public alors que d'autres ontologies accessibles ne sont pas directement applicables dans notre contexte. Par exemple, les ontologies liées à la gestion de crise ne peuvent pas être complètement réutilisées dans notre cas vu qu'une opération de secours diffère de la crise et de la réponse d'urgence à grande échelle dans de nombreux concepts. De plus, certains concepts importants liés à notre contexte ne sont pas bien définis dans les ontologies précédentes. Ajoutons à cela, dans notre travail, nous nous concentrons sur la modélisation des interactions et des opérations pour proposer un système de communication efficace, les aspects de communication sont donc importants. Par exemple, les concepts de communication tels que l'information doivent être liés aux tâches et aux acteurs. Dans la littérature, nous analysons qu'aucune des ontologies existantes ne considère ce point. Cependant, ces ontologies peuvent nous servir à emprunter des concepts généraux pour construire notre propre ontologie spécifique pour les communications dans les opérations de secours françaises.

A.3.4 Approches et ontologies pour la conception de systèmes et d’interfaces

La recherche sur la conception de systèmes et d’interfaces a évolué ces derniers temps. Plusieurs études ont proposé des approches basées sur les ontologies pour la conception de systèmes et d’interfaces utilisateur. Dans cette thèse, notre objectif principal est la conception d’interfaces utilisateur. Les approches de conception peuvent être classées en deux catégories. La première catégorie comprend des approches orientées vers la génération semi-automatique et la récupération d’interfaces utilisateur personnalisées basées sur des modèles et ontologies préalablement définis. L’idée principale ici est de présenter des interfaces personnalisées aux utilisateurs sur la base des modèles définis tels que les modèles de tâches ou d’utilisateurs. La deuxième catégorie comprend des approches de modélisation de contexte qui visent à développer et à récupérer des interfaces utilisateur basées sur des informations contextuelles telles que les capacités de l’appareil et la situation de contexte. Nous parlons ici d’interfaces utilisateur adaptatives, dynamiques et contextuelles. Bien que chaque approche ait son contexte et son domaine d’application, aucune d’elles n’est complète de manière à permettre aux utilisateurs finaux d’un système de communication collaboratif de concevoir le système et les interfaces de manière personnalisée. De plus, de multiples ontologies de conception de systèmes et d’interfaces ont été proposées dans la littérature. Le tableau 3.2 résume les ontologies analysées qui ont été créées pour formaliser les connaissances liées à la conception des systèmes et des interfaces. Malheureusement, certaines de ces ontologies ne sont pas accessibles au public alors que d’autres ontologies accessibles sont trop spécifiques aux solutions proposées. Cependant, ces ontologies peuvent servir pour réutiliser des concepts pour construire l’ontologie spécifique à la conception.

A.3.5 Approches et ontologies pour le contrôle d’accès

Il existe plusieurs définitions du contrôle d’accès. Chaque définition dépend du domaine d’application et du contexte d’utilisation. En sécurité informatique, le terme “contrôle d’accès” fait référence à l’utilisation de mécanismes permettant aux entités authentifiées d’effectuer des actions en fonction de leur niveau d’autorisation et d’empêcher les entités d’effectuer des actions non autorisées [Cheaito, 2012]. La recherche sur le contrôle d’accès et la gestion des droits d’accès

A.3 Ontologies et représentation des connaissances

à l'aide des technologies du web sémantique constitue un domaine intéressant pour de multiples chercheurs qui ont contribué et proposé plusieurs solutions dans ce contexte. Celles-ci ont abouti à la naissance de multiples langages Web sémantiques et cadres pour les politiques de contrôle d'accès. La recherche sur les technologies sémantiques et la représentation des connaissances ne s'est pas limitée au développement de langages et de cadres de politiques d'accès. Plusieurs études ont été menées pour développer et mettre en œuvre des modèles de contrôle d'accès à l'aide d'ontologies. D'autres études ont été menées pour gérer les droits d'accès dans des applications du monde réel grâce à l'utilisation d'ontologies. Dans ce contexte, un grand nombre d'ontologies liées au contrôle d'accès et à la gestion des droits d'accès ont été proposées dans la littérature. Certains chercheurs ont utilisé des ontologies pour représenter des modèles de contrôle d'accès tandis que d'autres ont cherché à utiliser des ontologies pour mettre en œuvre des solutions de gestion des droits d'accès. Le tableau 3.3 présente un résumé des ontologies analysées qui ont été développées pour formaliser les connaissances liées au contrôle d'accès et à la gestion des droits. Malheureusement, la plupart des ontologies proposées dans la littérature sont des ontologies ad-hoc développées pour des scénarios concrets, ce qui limite leur généralité et empêche leur réutilisation dans différents contextes [Imran-Daud *et al.*, 2016].

Comme il a été montré dans cette section, plusieurs approches basées sur l'ontologie pour la conception d'interfaces utilisateur ont été développées. Malheureusement, aucune de ces approches n'est complète de manière à permettre aux utilisateurs finaux d'un système de communication collaboratif de concevoir les spécifications et les interfaces du système de manière personnalisée. Dans cette conséquence, nous proposons dans cette thèse une approche pour identifier les spécifications du système et concevoir ses interfaces par ses utilisateurs finaux. L'approche proposée comprend l'intégration d'une politique de contrôle d'accès pour garantir l'accès confidentiel aux informations dans le système à développer. A cet effet, une plate-forme permettant de concevoir les interfaces et les spécifications du système de manière personnalisée est proposée. Suite à cette conception, les utilisateurs pourront se connecter, échanger et visualiser des informations dans le système conçu.

A.4 Modélisation des interactions

Comme on peut le voir sur la Figure A.1, la première étape de l'approche proposée consiste à analyser et modéliser les communications et les interactions dans ces opérations à travers l'étude des documents, rapports et législations liés au domaine. Cette étude nous permet d'identifier les différents services ainsi que leurs missions, d'analyser les procédures et de lier ces missions à des interactions. De plus, cette étude conduit à identifier les exigences, les critères et les besoins pratiques des acteurs sur la base de pratiques opérationnelles. De plus, cela permet de représenter ces procédures et interactions de manière formalisée. Dans cette section, nous présentons les acteurs principaux et les organisations qui participent dans les opérations de secours en France. De plus, nous présentons un modèle organisationnel. Ce modèle montre les différents niveaux organisationnels ainsi qu'un flux général d'informations et de décisions entre les différents niveaux. Ensuite, nous présentons les exigences et les paramètres principaux à considérer lors de la modélisation des interactions. Enfin, nous présentons un modèle de structure et un modèle d'interactions en se basant sur un scénario des opérations. Il est décrit sur la base d'une étude de la documentation liée au domaine, tel que des rapports ainsi que des études antérieures.

A.4.1 Secours à personne en France

Le secours à personne, en France, consiste à un ensemble de tâches précises à réaliser par des services publics afin de protéger des victimes et des patients en leur permettant d'échapper aux dangers, en sécurisant les lieux d'incidents et d'interventions, en appliquant des gestes de secourisme, et en assurant l'évacuation et le transport vers un lieu approprié de réception et d'hospitalisation [Diederichs *et al.*, 2006]. Plusieurs services sont impliqués et responsables des opérations de secours et de l'aide médicale urgente parmi lesquels on cite le Service d'Aide Médicale Urgente (SAMU) et le Service Départemental d'Incendies et de Secours (SDIS). L'état français a élaboré un rapport détaillé servant comme référentiel pour délimiter les missions et préciser les responsabilités [La DDSC et la DHOS, 2009; Richard-Hibon & Braun, 2009]. Le SAMU est chargé de fournir une aide médicale aux patients et aux victimes en : assurant une écoute médicale, choisissant des réponses adéquates avec la nature des appels, vérifiant la disponibilité des centres d'hospitalisation, préparant le transport et l'évacuation des victimes par les organisations de transport sanitaire et finalement, assurant

l'admission des victimes dans les centres d'hospitalisation. Alors que les SDIS sont responsables de la protection, la sécurisation, et la lutte contre les incendies. Ils sont également responsables de secours des patients et des victimes de catastrophes, ainsi que de leur évacuation. Ajoutons à cela, d'autres centres et services participent aux opérations de secours. Ils font partie des deux précédents et leurs tâches se limitent à la logistique tel que : la réception des appels et des alertes, le transfert des appels vers le service adéquat, l'assurance d'une bonne communication entre SDIS et SAMU, ainsi que la gestion des ressources. Chaque SDIS est composé de plusieurs centres et services qui gèrent des tâches et des fonctions distinctes. La Figure 4.2 illustre les différents services et centres qui composent un SDIS. Elle montre également la composition de ces centres et services. De même, chaque SAMU possède plusieurs centres et services qui gèrent des tâches et des tâches distinctes. La Figure 4.3 illustre différents services et centres qui composent un SAMU. Elle montre également la composition de ces centres et services.

A.4.2 Modèle organisationnel

Des interventions d'urgence et des opérations de secours efficaces nécessitent des structures d'intervention préétablies ainsi qu'une chaîne de commandement fiable et prédéfinie [Labba *et al.*, 2017]. De plus, pour mener à bien leurs opérations, les différents services et centres concernés doivent coopérer et communiquer pour accomplir leurs missions et devoirs à plusieurs niveaux organisationnels. Dans ce contexte, les services et centres multidisciplinaires impliqués dans les opérations de sauvetage françaises sont dispersés à différents niveaux de décision comme le montre le modèle d'organisation de la Figure 4.4. Comme le montre la Figure 4.4, dans le contexte français, la chaîne hiérarchique de commandement est composée de trois niveaux principaux : le niveau stratégique, le niveau tactique et le niveau opérationnel [Labba *et al.*, 2017; Saoutal *et al.*, 2014]. Dans le cas des opérations de secours à petite échelle, qui constituent le point d'intérêt de notre travail, la plupart des opérations et des communications se déroulent à deux niveaux seulement : le niveau tactique et opérationnel. Alors que l'implication du niveau stratégique est limitée aux opérations à grande échelle telles que la gestion de crise. Ainsi, nous avons concentré nos travaux sur l'analyse et la modélisation des communications et des interactions entre les niveaux tactique et opérationnel.

A. RÉSUMÉ DE LA THÈSE

Après avoir identifié les organisations et acteurs impliqués dans les opérations de secours françaises, il est important d'analyser leurs tâches et interactions dans un scénario d'opération. Pour cela, nous avons décrit un scénario d'opération. Ce scénario est détaillé dans la section 4.2.3. Il constitue une base d'analyse et de modélisation des pratiques et des interactions. Il a été défini sur la base des rapports existants et des documents liés au domaine. Malgré que scénario proposé se limite aux opérations de secours en France, ce dernier se caractérise par sa généralité puisqu'il ne se limite pas à un type d'accident particulier.

A.4.3 Modélisation des interactions et des communications

Avant de modéliser les interactions, il faut identifier les exigences de modélisation et les composants du modèle. Par conséquent, nous proposons plusieurs exigences pour la modélisation des interactions. Ensuite, nous proposons un modèle structurel basé sur ces exigences. Finalement, nous fournissons un modèle d'interaction sur la base du scénario décrit dans 4.2.3.

A.4.3.1 Exigences pour la modélisation des interactions

Avant de créer un modèle tel que des modèles d'interaction ou d'information, il est indispensable de définir les exigences de modélisation et les éléments constitutifs du modèle. L'objectif principal de notre modèle est d'étudier et de représenter les interactions et la communication dans les opérations de secours, puis de développer un système visant à soutenir la communication afin de renforcer la prise de conscience des situations. En ce qui concerne la prise de conscience, qui est l'intérêt principal de notre travail, assurer un niveau élevé de prise de conscience d'une situation nécessite de percevoir tous les éléments de cette situation dans un volume de temps et d'espace, ainsi que de comprendre leurs significations et leurs relations. En plus de cela, soutenir la communication et l'interaction nécessite d'identifier toutes les informations pertinentes qui renseignent sur une situation. Par conséquent, définir les éléments de la situation et les informations importantes est la première étape vers la prise de conscience. Ce sont les principaux éléments à prendre en compte lors de la modélisation des interactions et des processus. Le premier élément à considérer est les acteurs (Actors) et leurs rôles (Roles) ainsi que leurs positions (Positions) dans le modèle organisationnel. Le deuxième élément est les activités et les actions exécutés par

l'acteur. Les actions et activités sont représentées en tant que tâches (Tasks) dans notre modèle. Un autre élément est l'information (Information). C'est la base pour la communication et la conscience des situations. De plus, le partage de ces informations nécessite l'utilisation d'un outil de communication. Il est donc également essentiel de définir l'instrument de communication (Communication Instrument) utilisé pour acheminer la communication. Cette définition peut aider à spécifier où et quand cette assistance est requise avec son type. En outre, les acteurs participant à une seule opération de secours sont séparés géographiquement. Par conséquent, les tâches, opérations et communications se déroulent dans des espaces différents. Pour cette raison, il est nécessaire de différencier les différents espaces (Location) lors de la modélisation. Finalement, étant que les opérations de secours sont des situations dynamiques évoluant avec le temps, la prise en compte du paramètre Temps (Time) revêt une grande importance. Cette dynamique affecte l'état de tous les autres éléments tels que les informations de situation ou les tâches. Cependant, modéliser un processus complexe dans le temps est une tâche ardue. Des études [Nunavath & Prinz, 2015] montrent que la modélisation de processus ou d'interactions dynamiques et complexes, tels que la gestion des urgences ou le secours, nécessite de scinder ces processus en plusieurs phases et de les séparer dans le temps. Ainsi, nous divisons une opération de secours en phases principales séparées composées chacune de plusieurs sous-phases et nous présentons ces phases sur une chronologie, comme le montre la Figure 4.6. Ajoutons à cela, le fait de diviser une opération complète en phases en fonction du temps, paramètre principal dans le secours, facilite la modélisation des processus et des activités et par suite les interactions par rapport à ces phases. En fonction de l'évolution du temps, une opération de secours peut être divisée en six phases principales : Phase d'alerte (Alerte phase), Implication des moyens et des personnes adaptés (Involvement of adapted means and persons), départ des secouristes (Departure of rescuers), Opérations sur site (On-Site Operations), Evacuation et transport des victimes (Victims' evacuation and transportation), et enfin, Phase de retour et fin (Return and end phase).

A.4.3.2 Modèle d'interactions dans le secours

Il existe ici plusieurs approches et techniques pour représenter et formaliser des processus, des activités et des interactions. Certaines techniques sont basées sur des modèles et des diagrammes de processus métier tandis que d'autres sont dérivées d'approches multi-agents. Dans cette thèse, nous choisissons d'adopter

A. RÉSUMÉ DE LA THÈSE

l'approche basée sur la modélisation des processus métier en étendant les diagrammes UML pour de nombreuses raisons. La première raison est que les modèles de processus et les diagrammes peuvent être utilisés pour modéliser des processus dynamiques, des interactions et des séquences en tenant compte de plusieurs paramètres. La deuxième raison est que les modèles de processus métier permettent la représentation des flux d'informations entre différents acteurs, ce qui est important pour la modélisation des interactions. Finalement, la troisième raison est que les diagrammes UML sont précis, et destinés à décrire les spécifications d'un système d'information, ce qui répond à nos besoins puisque notre objectif est de concevoir un système de communication opérationnel. Cependant, aucun des diagrammes UML existants ne permet de représenter les interactions dans un seul modèle en prenant en compte tous les paramètres précédemment définis. À cette fin, nous faisons un mélange de diagramme de collaboration UML, de diagramme d'activité UML et de diagramme de séquence UML [Glasse, 2008] pour représenter clairement notre modèle dans un diagramme comme le montre le modèle de structure illustré dans la Figure 4.7.

Après avoir défini les éléments requis pour constituer un modèle d'interaction dans les opérations de secours et créé un modèle de structure, nous passons à la dernière étape, qui consiste à construire un modèle d'interaction pour les opérations de secours. Pour cela, nous avons pris l'exemple d'un incident causant une ou plusieurs victimes et nécessitant l'engagement de plusieurs acteurs de différentes organisations. Munis de leurs véhicules et de leur matériel, ces acteurs doivent accéder aux sites d'intervention, sécuriser des lieux, protéger les victimes, récupérer des informations et les échanger avec les décideurs, mener et exécuter des actions appropriées, puis évacuer et transporter les victimes vers un lieu d'hospitalisation. Le modèle d'interaction proposé est présenté dans les Figures 4.8 à 4.20. À partir du modèle présenté, nous pouvons voir comment les acteurs impliqués interagissent les uns avec les autres en fonction des actions et de la situation. De plus, nous pouvons voir les informations nécessaires ou produites à chaque étape avec l'instrument utilisé pour les échanger. Ajoutons à cela, nous pouvons facilement extraire les dépendances entre l'acteur, l'action, l'information, l'instrument de communication, la phase d'opération, l'emplacement et le temps. De plus, on peut simplement voir le flux d'informations entre le niveau opérationnel et le niveau tactique dans les opérations de sauvetage. De même, ce modèle sert de base pour définir les spécifications du système de communication à partir des

protocoles de communication définis dans les opérations de secours et ainsi, pour supporter la représentation des situations. Cependant, il ne couvre pas toutes les incertitudes qui peuvent survenir en termes d'activités et d'informations car la plupart de ces incertitudes ne peuvent être prédites dans les protocoles susmentionnés.

A.5 Ontologie ResOnt

Après avoir modélisé les interactions, passons à l'étape suivante de l'approche présentée dans la section [A.1.1](#). Cette deuxième étape s'inscrit dans la construction d'une ontologie d'application qui représente les connaissances nécessaires à la conception d'un système de communication orienté vers les acteurs du secours qui garantit la confidentialité des informations. Afin de proposer un système utilisable basé sur des pratiques opérationnelles, nous développons cette ontologie à partir du modèle d'interaction présenté dans la section [A.4](#).

Lors de la conception d'un système de communication orienté pour les acteurs du secours, plusieurs aspects et dimensions doivent être pris en compte. Premièrement, étant donné que le système est orienté pour soutenir l'échange d'informations et la conscience mutuelle, il est essentiel de prendre en compte les différentes pratiques et interactions ainsi que les éléments nécessaires pour soutenir la conscience. Deuxièmement, il est fortement nécessaire de prendre en compte la conception et l'utilisation du système dans les pratiques réelles. Troisièmement, étant donné qu'une grande quantité d'informations échangées dans les opérations de secours sont des informations personnelles, il est nécessaire d'envisager un accès confidentiel aux informations. Ainsi, nous proposons l'ontologie ResOnt qui couvre ces aspects. Dans cette section, nous présentons l'ontologie ResOnt ainsi que la méthodologie adoptée pour son développement. L'ontologie ResOnt constitue un élément essentiel de la démarche proposée. Elle aide à développer un système qui répond aux critères identifiés en :

- Assurant une représentation commune des informations entre les différentes parties prenantes. Cela aidera à assurer une représentation et une compréhension communes et partagées des situations entre les parties prenantes, ce qui améliorera la connaissance de la situation.
- Représentant et formalisant différentes procédures et flux d'informations. Grâce à cette représentation, ResOnt contribuera à développer un système

A. RÉSUMÉ DE LA THÈSE

basé sur les pratiques et les interactions entre les parties prenantes en tenant compte de la diversité de leurs besoins.

- Représentant les connaissances nécessaires pour gérer les droits d'accès et garantir un accès confidentiel aux informations dans le système. Cela contribuera à garantir la confidentialité des informations.
- Représentant les connaissances requises pour la conception et la configuration dynamiques du système et des interfaces. Cela facilitera la flexibilité et l'adaptabilité du système aux différents usages. De plus, cette représentation constitue une étape essentielle vers la personnalisation des interfaces système.

Dans ce contexte, nous proposons de construire l'ontologie ResOnt basée sur trois modules différents. De plus, nous interconnectons ces trois modules via de multiples relations afin d'obtenir l'ontologie complète de l'application ResOnt. Nous remarquons que les modules mentionnés ci-dessus sont interdépendants. Le but de cette modularisation se limite à la séparation et à la classification de différents concepts et relations basés sur des domaines et des aspects distincts. Les modules d'ontologie sont :

- **ResOnt Rescue and Communication** : Ce module intègre les concepts et les relations nécessaires pour formaliser les pratiques et les interactions dans les opérations de secours. Il sert également à assurer une compréhension partagée des situations entre les différentes parties prenantes.
- **ResOnt Design** : Ce module comprend les concepts et les relations nécessaires pour concevoir un système de communication de manière flexible et personnalisée.
- **ResOnt Access Control** : Ce module comprend les concepts et les relations nécessaires pour contrôler l'accès gérer les droits d'accès.

A.5.1 Méthodologie de développement

Dans ce travail, nous adoptons la méthodologie METHONTOLOGY pour développer l'ontologie proposée [Fernández-López *et al.*, 1997]. Ce choix est soutenu par le fait que cette dernière est la plus mature parmi les méthodologies existantes [Corcho *et al.*, 2003]. La Figure 5.1 montre les principales activités et

étapes du développement de l'ontologie telles que définies dans METHONTOLOGY.

A.5.1.1 Spécification

Dans cette thèse, nous adoptons les questions de compétence (CQ) comme technique pour définir les spécifications de l'ontologie. Les questions de compétence jouent un rôle important dans le cycle de vie du développement de l'ontologie car elles représentent les exigences de l'ontologie [Bezerra *et al.*, 2013]. Elles consistent en un ensemble de questions énoncées en langage naturel auxquelles l'ontologie doit pouvoir répondre [Noy & Hafner, 1997]. Pour plus de clarté et de simplicité, nous classons les questions de compétence définies dans ResOnt en trois catégories: (1) les CQs liées aux pratiques et interactions dans les opérations de secours; (2) les CQs liées à la conception du système et des interfaces; (3) Les CQs liées au contrôle d'accès. Nous commençons par des questions liées aux pratiques et aux interactions dans les opérations de secours. Dans ce contexte, nous avons défini un total de trente-deux questions de compétence présentées dans le tableau 5.2. Ces questions ont été principalement définies sur la base du modèle d'interaction décrit dans la section A.4. De plus, nous avons défini plusieurs questions liées à la conception du système et des interfaces. Dans ce contexte, onze questions ont été définies et présentées dans le tableau 5.3. Finalement, nous avons défini plusieurs questions de compétence liées au contrôle d'accès et à la gestion des droits. Au total, quatre questions ont été définies dans ce contexte, comme indiqué dans le tableau 5.4.

A.5.1.2 Acquisition de connaissances

Cette phase consiste à acquérir des connaissances en utilisant conjointement des techniques telles que l'analyse formelle et informelle de textes, des entretiens, des brainstormings et des outils d'acquisition de connaissances. Malheureusement, dans ce travail, nous n'avons pas eu l'opportunité de rencontrer des experts du domaine censés aider dans l'acquisition des connaissances et les étapes d'évaluation de l'ontologie. Par conséquent, nous proposons de développer l'ontologie requise basée sur la documentation relative au domaine ainsi que sur les ontologies existantes. Pour ce faire, une analyse approfondie du domaine de secours a été réalisée à partir de documents, rapports, législations et ontologies liés au domaine. De plus, nous avons analysé les interactions et les pratiques à partir du modèle d'interaction présenté dans la section A.4. D'autre part, nous avons mené une

A. RÉSUMÉ DE LA THÈSE

étude des approches et des ontologies existantes liées à la conception de systèmes. De même, plusieurs études et ontologies existantes liées au contrôle d'accès ont été analysées pour capter les connaissances requises dans ce contexte. Ces études nous ont permis d'acquérir une connaissance spécifique et détaillée des concepts requis, de leurs propriétés et de leurs relations.

A.5.1.3 Conceptualisation

La conceptualisation consiste à structurer la connaissance du domaine dans un modèle conceptuel ou une ontologie conceptuelle. Ce dernier vise à décrire les connaissances liées à un certain domaine en termes de vocabulaire de domaine identifié dans l'activité de spécification d'ontologie [Fernández-López *et al.*, 1997]. Dans un premier temps, nous avons identifié trois modules pour représenter les connaissances liées à chaque partie de la conception d'un système de communication et personnalisé orienté vers les acteurs du secours qui garantit la confidentialité des informations. Ensuite, nous avons défini les concepts requis dans chaque module sur la base des connaissances acquises à partir des documents, des ontologies existantes et de la documentation relative aux domaines. De plus, pour créer une ontologie d'application complète, il est nécessaire de définir des relations au sein et entre les différents modules et d'intégrer les trois modules définis. Pour cela, nous proposons de créer un module commun appelé ResOnt Common comme cela a été fait dans [Elmhadhbi *et al.*, 2019] et suggéré dans [Özacar *et al.*, 2011]. Le module commun proposé incorpore les concepts généraux utilisés par différents modules. Il peut alors être spécifié pour construire les trois modules séparément. La Figure 5.2 illustre les modules de l'ontologie ResOnt.

Dans le but d'accélérer et d'améliorer le développement d'une ontologie, Fernández-López *et al.* [1997] suggère de réutiliser les ontologies existantes au lieu de partir de zéro. Par conséquent, nous proposons de réutiliser une ontologie de haut niveau et une ontologie de niveau intermédiaire comme une étape essentielle pour créer une ontologie réutilisable qui peut être interopérable ou réutilisable par d'autres ontologies. Dans ce contexte, nous proposons la réutilisation de BFO comme ontologie de premier niveau car elle est universelle et réaliste [Dumontier & Hoehndorf, 2010]. La Figure 5.3 montre la hiérarchie is-a de BFO dans sa version: 2.0. implémenté en utilisant le langage OWL-2. Concernant les ontologies de niveau intermédiaire, nous choisissons de réutiliser les ontologies CCO. La raison du choix de CCO est double. D'une part, CCO étend le framework d'ontologie de premier niveau BFO. Le framework BFO incorpore l'ontologie

BFO qui est l'ontologie de premier niveau sélectionnée dans notre cas. De plus, ce framework inclut l'ontologie des relations (RO) qui définit les relations entre les concepts à un niveau élevé. D'autre part, grâce à ses multiples ontologies, CCO peut être simplement étendu pour créer une ontologie d'application qui couvre des aspects et des domaines distincts. La Figure 5.4 montre les différentes ontologies et la structure d'importation dans CCO. Sur la base de cette sélection, nous avons importé les modules de CCO et nous avons créé le module commun de ResOnt. Suite à cette création, nous définissons différentes relations au sein et entre les modules et nous intégrons les modules créés pour construire l'ontologie d'application complète ResOnt. La Figure 5.5 illustre différents modules et la stratégie d'importation adoptée pour créer l'ontologie ResOnt.

En plus de l'utilisation d'ontologies de niveau supérieur et intermédiaire, Fernández-López *et al.* [1997] recommande la réutilisation des ontologies de domaine existantes, le cas échéant. Dans la section A.3, une analyse des ontologies existantes liées aux trois domaines d'intérêt a été présentée. Un grand nombre d'ontologies ont été proposées dans la littérature dans le contexte des interventions d'urgence et de secours, de la conception des systèmes et des interfaces, du contrôle d'accès et de la gestion des droits. Malheureusement, la majorité de ces ontologies ne sont pas accessibles au public, tandis que d'autres sont des ontologies ad hoc orientées pour des cas d'utilisation spécifiques. Par conséquent, nous ne pouvons pas réutiliser complètement ces ontologies. Cependant, nous réutilisons certains concepts et relations définis dans ces ontologies.

A.5.1.4 Formalisation et implémentation

L'activité de formalisation et d'implémentation consiste à transformer une ontologie conceptuelle en une ontologie formelle [Park *et al.*, 2008]. Dans ce contexte, nous avons implémenté l'ontologie ResOnt en utilisant le langage OWL-2 dans le logiciel Protégé [Musen, 2015]. La Figure 5.6 montre les spécifications et les métriques de l'ontologie ResOnt après son implémentation dans Protégé.

A.5.1.5 Évaluation

Plusieurs études ont été menées dans la littérature pour analyser les problèmes d'évaluation des ontologies [Brank *et al.*, 2005; Hlomani & Stacey, 2014; Vrandečić, 2009]. Selon [Brank *et al.*, 2005], les approches d'évaluation d'ontologie

A. RÉSUMÉ DE LA THÈSE

peuvent être classées en : Évaluation Gold Standard, Évaluation basée sur les applications ou les tâches, Évaluation basée sur les données, Évaluation effectuée par l'utilisateur. Selon [Hlomani & Stacey, 2014], l'approche effectuée par l'utilisateur permet une évaluation meilleure et plus complète par rapport aux autres approches. Malheureusement, au cours de cette thèse, nous n'avons pas pu rencontrer un expert du domaine après le développement de l'ontologie pour l'évaluer. Par conséquent, nous ne pouvions pas adopter cette approche. Cependant, nous proposons d'adopter une approche applicative pour évaluer ResOnt. Pour cela, nous allons instancier l'ontologie et la valider à travers la plateforme et la politique de contrôle d'accès qui seront présentées dans la section [A.6](#).

A.5.1.6 Maintenance

L'activité de maintenance enrichit et corrige l'ontologie si nécessaire [Corcho *et al.*, 2005]. Cette activité suit la phase d'évaluation et constitue la dernière phase du cycle de développement de l'ontologie. Sur la base de sa méthodologie de développement, ResOnt peut être modifié selon deux formes de changement: la spécification et les changements conceptuels. Dans ce contexte, de nouveaux concepts, relations ou même d'autres ontologies peuvent être intégrés dans ResOnt. De plus, de nouveaux attributs peuvent être ajoutés aux concepts de ResOnt. Puisque ResOnt est toujours dans sa première version, elle n'a fait l'objet d'aucune modification.

A.5.2 Description de l'ontologie ResOnt

Après avoir réutilisé l'ontologie BFO ainsi que les ontologies de CCO, nous avons défini les concepts nécessaires dans chaque module de ResOnt. Cette définition est basée sur la documentation ainsi que plusieurs ontologies existantes. Suite à cela, nous avons obtenu trois arbre hiérarchique qui ne contiennent que des relations is-a (est-un).

A.5.2.1 Module ResOnt Rescue and Communication

Comme déjà mentionné, ce module comprend les concepts liés aux pratiques, communications, et interactions dans le secours à personne. Les concepts principaux définis dans ce module sont : *Organization*, *Organization Member*, *Organization Member Role*, *Communication Instrument*, *Incident*, *Intervention*, *Victim*, *Group of information*, *Information*, *Material*, *Task*, *Phase*, et *Sub Phase*. La Figure [A.2](#)

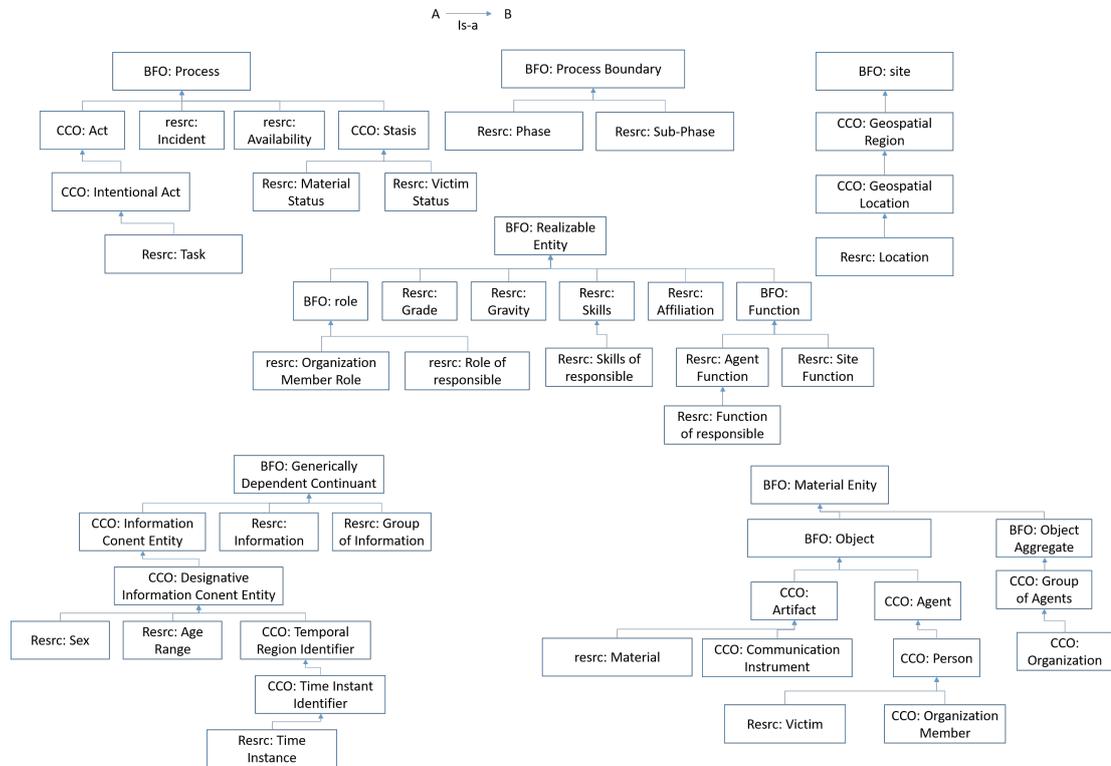


Figure A.2: Hiérarchie du module ResOnt Rescue and Communication.

montre la classification des concepts définis dans le module Rescue and Communication.

A.5.2.2 Module ResOnt Design

Ce module comprend principalement les concepts liés à la conception du système et ses interfaces. En ce qui concerne la conception des systèmes et des interfaces, plusieurs aspects et paramètres doivent être pris en compte. Certains de ces paramètres sont liés au système lui-même, comme l'interface et ses dimensions. D'autres paramètres sont liés aux informations telles que le type de données, l'orientation, le degré de criticité et la catégorie. Alors que le troisième type de paramètres est lié aux fonctionnalités et aux interactions dans le système. Les concepts principaux définis dans ce module sont : *Data type*, *Orientation*, *Interaction way*, *degree of Criticality*, *Field Type*, *Informational Component*, *Media Component*, *Interface*, *Dimension*, et *Functionality*. La Figure A.3 montre la classification des concepts définis dans le module ResOnt Design.

A. RÉSUMÉ DE LA THÈSE

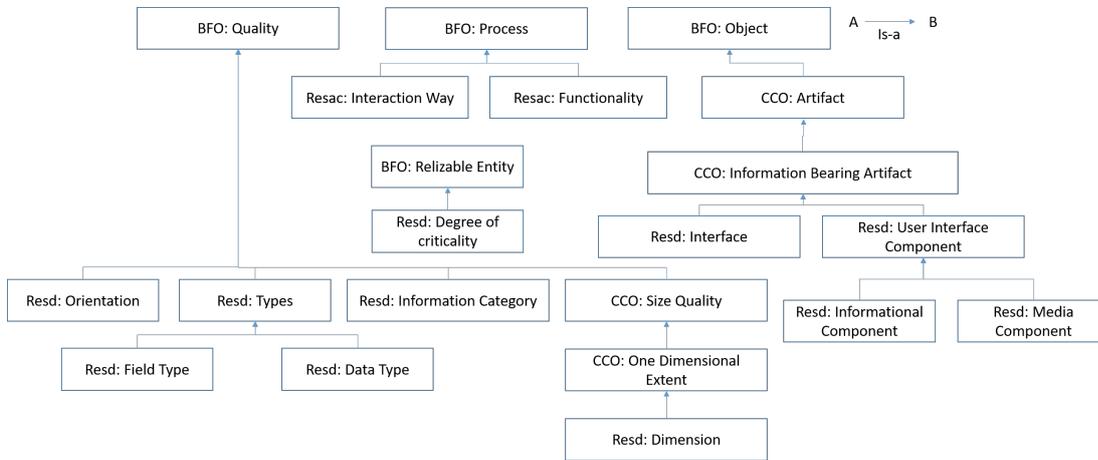


Figure A.3: Hiérarchie du module ResOnt Design.

A.5.2.3 Module ResOnt Access Control

L'objectif du module de contrôle d'accès dans ResOnt est de définir les droits d'accès d'un agent sur un certain groupe d'informations. De plus, il sert de base de connaissances pour déterminer le type d'accès s'il est interdit ou autorisé en fonction de plusieurs paramètres. Tandis que d'autres fonctions requises pour contrôler l'accès sont implémentées dans le système final. Les concepts principaux définis dans ce module sont : *Action* et *Access Type*. D'autres concepts nécessaires pour le contrôle d'accès tel que *Group of information*, *Organization member role*, *Task*, et *Functionality* ont été déjà définis dans les deux autres modules. La Figure A.4 montre la classification des concepts définis dans le module ResOnt Access Control.

A.5.2.4 Ontologie ResOnt complète

Après avoir défini les concepts principaux de chaque module, nous relierons les concepts au sein et entre les modules grâce à plusieurs propriétés. La définition des relations entre les concepts ontologiques est essentielle pour obtenir un modèle conceptuel complet pouvant être spécifié à partir des instances de l'ontologie. En conséquence, nous avons classé ces relations en :

- **Operational properties:** Comprennent les différentes relations qui relient les concepts liés aux communications et aux pratiques. La Figure A.5 montre un graphe conceptuel qui illustre une vue partielle des relations opérationnelles entre différents concepts.

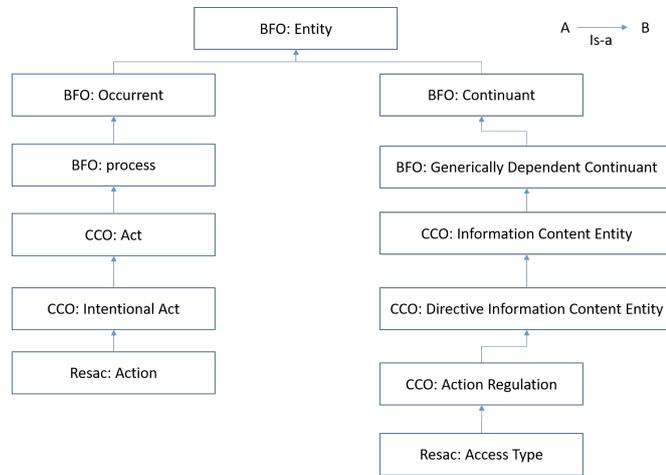


Figure A.4: Hiérarchie du module ResOnt Access Control.

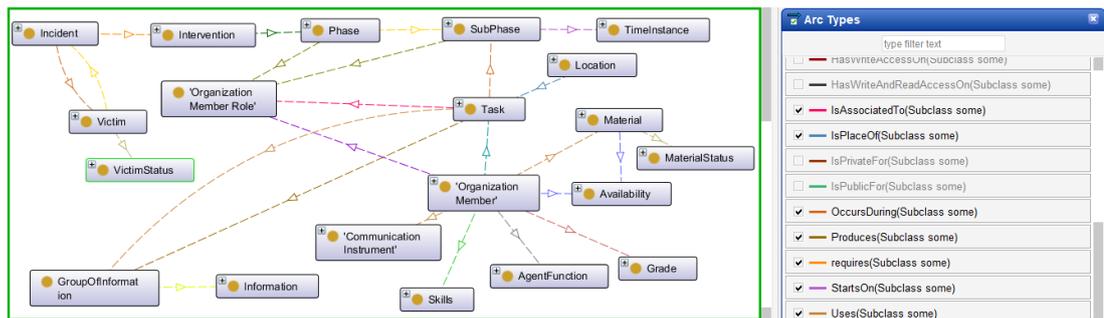


Figure A.5: Graphe conceptuel lié aux communications et aux pratiques.

- **Design properties:** Incluent différentes relations requises liées à la conception des systèmes et des interfaces. La Figure A.6 illustre un graphe conceptuel qui montre une vue partielle des propriétés de conception entre différents concepts.
- **Access properties:** Comprennent différentes relations requises pour assurer le contrôle d'accès et la gestion des droits. La Figure A.7 représente un graphe conceptuel qui illustre une vue partielle des propriétés de contrôle d'accès entre différents concepts.

A.6 Plateforme de support à l'awareness

Après avoir modélisé les interactions et créé une ontologie applicative, passons aux troisième et quatrième étapes de l'approche présentée dans la section A.1.1. La troisième étape réside dans le développement d'une plateforme orientée vers les acteurs du secours. Par conséquent, nous concevons et développons une plateforme basée sur le modèle d'interaction présenté dans la section A.4 et l'ontologie ResOnt présentée dans la section A.5. Grâce à cette plateforme, les utilisateurs finaux pourront définir les spécifications liées à l'information. De plus, chaque utilisateur pourra concevoir son interface graphique de manière personnalisée en fonction de son contexte. Sur la base de ces spécifications et de cette conception, les utilisateurs finaux pourront se connecter au système final afin d'échanger des informations d'une manière efficace. Quant à la quatrième étape, elle consiste à garantir un accès confidentiel à l'information grâce à des mécanismes de contrôle d'accès et de gestion des droits. Par conséquent, nous proposons une politique de contrôle d'accès pour renforcer la confidentialité de l'information. Pour cela, nousinstancions l'ontologie proposée afin d'être utilisée dans la plateforme proposée. Dans cette section, nous présentons la plateforme précitée, ainsi que la politique de contrôle d'accès et de gestion des droits proposée.

A.6.1 Principes de base

En se basant sur les solutions proposées dans la section A.1.1, la plateforme proposée doit répondre à trois principes de bases comme le montre la Figure 6.1. Ces principes sont: Identification du contexte, Configuration et conception dynamiques et personnalisées, Communication et contrôle d'accès.

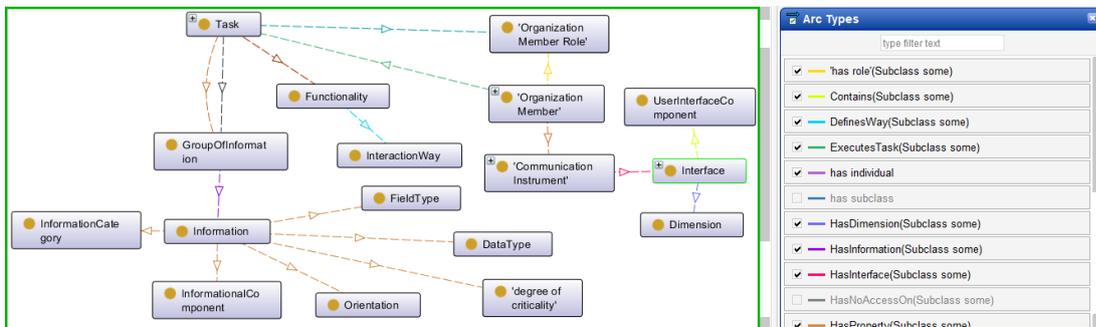


Figure A.6: Graph conceptuel lié à la conception de systèmes et d'interfaces.

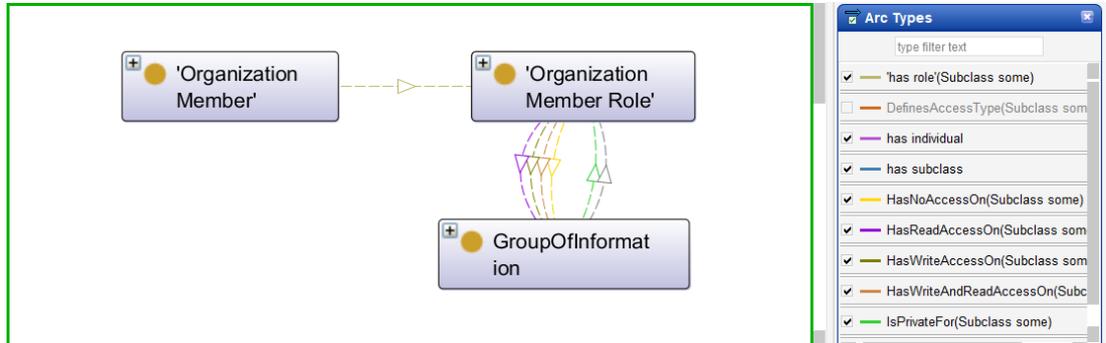


Figure A.7: Graphique conceptuel lié au contrôle d'accès et à la gestion des droits.

- **Identification du contexte :** Différents acteurs sont impliqués dans les opérations de secours. Chaque acteur a ses missions et ses responsabilités. De plus, chaque acteur exécute plusieurs tâches en fonction de son contexte. Le contexte d'un acteur comprend la phase d'intervention, la sous-phase, le rôle et l'emplacement de l'acteur ainsi que l'instrument de communication utilisé. De plus, chaque tâche peut nécessiter ou générer un ou plusieurs groupes d'informations où chaque groupe possède plusieurs informations. Par conséquent, il est nécessaire de déterminer quelles informations sont nécessaires pour améliorer la conscience de la situation d'un acteur en fonction de son contexte. Ainsi, le premier principe de la solution proposée consiste à identifier et créer le contexte d'usage. Cette étape aboutit à la détermination des groupes d'informations et d'éléments d'information nécessaires à la prise de conscience dans un certain contexte d'utilisation.
- **Configuration et conception dynamiques et personnalisées :** Chaque utilisateur du système a des exigences spécifiques en fonction de son contexte et de ses préférences. Ajoutons à cela, les systèmes de communication orientés vers les opérations de secours font l'objet de modifications continues. Par exemple, les concepts de domaine tels que les rôles des membres de l'organisation peuvent être modifiés avec le temps. Par conséquent, le système doit être flexible à toute modification selon les besoins. De plus, il est fortement nécessaire de permettre aux utilisateurs finaux de définir les spécifications du système et de concevoir les interfaces graphiques de manière dynamique et personnalisée. Dans ce contexte, ces utilisateurs devraient pouvoir configurer les spécifications du système. Nous remarquons que les spécifications du système intègrent différents paramètres liés aux in-

A. RÉSUMÉ DE LA THÈSE

formations telles que Data Type, Informational Component, Field Type et d'autres paramètres. De plus, chaque utilisateur doit être capable de concevoir les interfaces graphiques du système en fonction des contextes créés. Cette étape se traduit par un système de communication personnalisé et flexible qui gagnera l'acceptabilité de ses utilisateurs finaux.

- **Communication et contrôle d'accès** : Afin de soutenir la conscience mutuelle, les acteurs du secours doivent être capables de communiquer efficacement en transmettant, recevant et visualisant des informations en fonction de leurs contextes. Cependant, une grande partie des informations échangées lors des opérations de secours sont des informations personnelles et sensibles. Dans ce contexte, il est fortement demandé d'interdire tout accès externe à ces informations. De plus, en fonction de leurs rôles et de leurs tâches, les acteurs participants devraient avoir différents droits d'accès à l'information. Par conséquent, l'accès à l'information devrait être contrôlé et limité aux personnes autorisées. Les mécanismes de contrôle d'accès et de gestion des droits conviennent pour maintenir l'accès aux informations et surveiller les actions des utilisateurs légitimes en médiatisant toute tentative de l'utilisateur d'accéder à une ressource dans le système [Abomhara *et al.*, 2016]. Ainsi, le troisième principe consiste à assurer des communications confidentielles en intégrant des mécanismes de contrôle d'accès et de gestion des droits dans le système de communication. Le résultat de cette étape est un système qui garantit un accès confidentiel aux informations.

A.6.2 Fonctionnalités et architecture

Afin de respecter les principes de base, nous proposons plusieurs fonctionnalités que la plateforme à ses utilisateurs finaux. Les principales fonctionnalités sont: (1) Création de contexte; (2) Configuration des éléments de contexte; (3) Vérifier quelles sont les tâches associées à l'utilisateur en fonction de son contexte; (4) Vérifier quels sont les groupes d'informations et donc les informations dont un utilisateur dispose dans un contexte; (5) Configurer les spécifications du système et les propriétés d'information sur la base d'un ensemble de propriétés proposées et de valeurs possibles; (6) Créer de templates personnalisés liés aux contextes et aux identités des utilisateurs; (7) Ajout des composants multimédias requis aux interfaces utilisateur; (8) Positionnement des différents composants

d'information et des composants multimédias dans les templates créés; (9) Connexion au système final après sa conception; (10) Créer, transmettre, recevoir et visualiser des informations tout en respectant la politique de contrôle d'accès. Dans la section A.5, nous avons présenté plusieurs modèles conceptuels basés sur les relations entre différents concepts définis dans l'ontologie. Après avoir créé les modèles conceptuels, il est nécessaire d'instancier cette ontologie. De plus, il est essentiel d'identifier les différentes relations entre ces instances. L'importance de cette instanciation et de ces relations est de pouvoir créer une base de connaissances complète à travers laquelle il sera possible de faire les inférences requises. Par exemple, sur la base de ces instances, des valeurs possibles peuvent être proposées à l'utilisateur pendant la phase de conception ainsi que pendant l'utilisation du système de communication. En conséquence, nous instancions les concepts liés aux interactions et nous définissons les relations entre eux sur la base du modèle d'interaction présenté dans la section A.4. De plus, nous instancions des concepts liés à la conception d'interfaces en attribuant un ensemble de valeurs possibles à chaque concept. De même, les concepts requis pour le contrôle d'accès sont instanciés et liés afin d'utiliser la politique de contrôle d'accès et de gestion des droits. À l'issue de cette étape, nous obtenons une base de connaissances ontologiques que l'on peut interroger pour assurer les différentes fonctionnalités de la plateforme. Nous remarquons que certaines fonctionnalités nécessitent l'utilisation d'une base de connaissances. Alors que d'autres fonctionnalités reposent sur l'utilisation d'une base de données pour stocker des informations dynamiques telles que celles échangées dans le système final ou des informations d'identification utilisateur requises pour authentifier les utilisateurs. Afin de manipuler les différentes fonctionnalités, nous avons proposé de concevoir la plateforme comme le montre la Figure A.8 qui montre l'architecture générale et les principaux composants de la plateforme proposée. Ces composants sont : Le front-end, le Back-end, la base de connaissances et la base de données.

A.6.3 Identification du contexte

L'identification du contexte représente la première activité principale à réaliser par les utilisateurs finaux du système. Il est essentiel d'identifier les différents contextes afin de déterminer les besoins en termes d'information. La Figure 6.3 illustre un diagramme de cas d'utilisation pour l'identification du contexte. Comme nous pouvons le voir dans la Figure 6.3, l'activité d'identification de contexte se compose de deux sous-activités qui sont: (1) Création de contexte; et (2)

A. RÉSUMÉ DE LA THÈSE

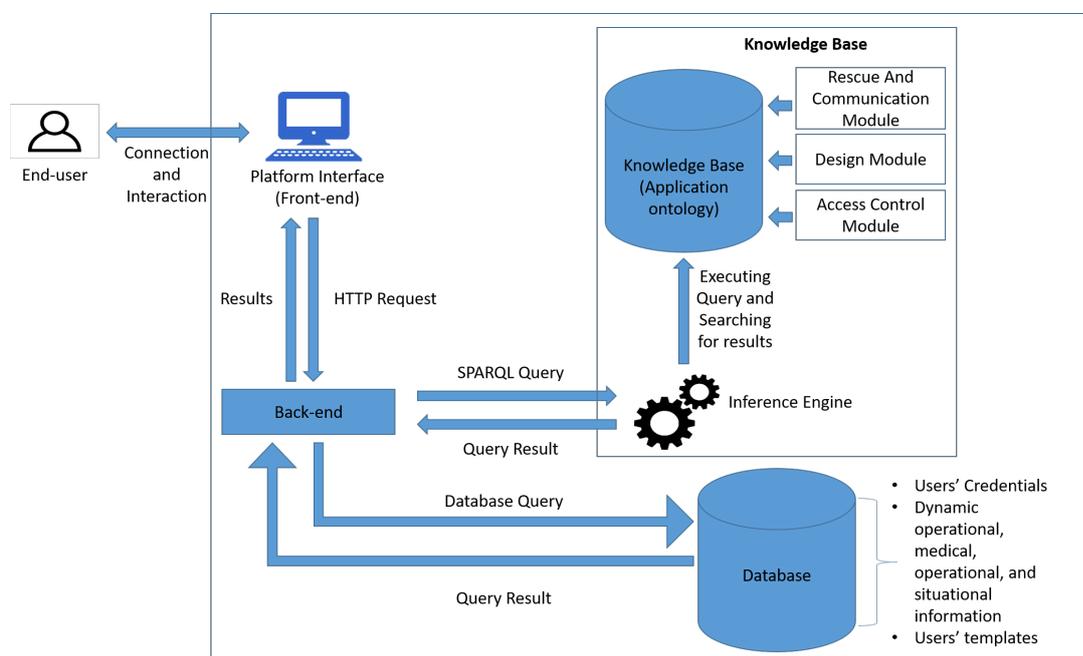


Figure A.8: Architecture générale de la plateforme proposée.

Création de tâches. La création de contexte est la procédure de génération de contextes spécifiques en attribuant des valeurs spécifiques à chacun des éléments de contexte. Dans ce cas, certains paramètres doivent être déterminés automatiquement dans la solution proposée, tels que le rôle et l'ID de l'utilisateur en fonction du processus d'authentification. Au contraire, d'autres éléments de contexte sont configurés par l'utilisateur final lui-même. Afin de faciliter les tâches des utilisateurs finaux dans l'activité de création de contexte, ils doivent être en mesure de configurer ces éléments en fonction d'un ensemble de valeurs proposées. Par conséquent, nous proposons de définir ces valeurs comme des instances de concepts dans l'ontologie ResOnt. La Figure 6.4 illustre un diagramme de séquence pour l'activité de création de contexte. Concernant la création de tâches, cette activité consiste à vérifier quelles sont les tâches associées à l'utilisateur en fonction de son contexte, à vérifier quels sont les groupes d'informations et donc les informations produites ou nécessaires pour réaliser chaque tâche dans le contexte, supprimer un groupe d'informations ou d'informations provenant d'une tâche spécifique, déterminer les groupes d'informations et informations nécessaires dans un contexte après la configuration de différentes tâches. Afin de garantir les fonctionnalités requises dans l'activité de création de tâche, il est nécessaire d'instancier l'ontologie et de relier ces instances. Par exemple,

différentes tâches, groupes d'informations et informations doivent être définis dans la base de connaissances. Par conséquent, nous avons instancié différents concepts qui représentent des tâches, des groupes d'informations et des informations et les avons liés. La Figure 6.9 illustre un diagramme de séquence pour l'activité de création de tâche.

A.6.4 Configuration et conception dynamiques et personnalisées

La configuration dynamique des spécifications et la conception personnalisée des interfaces représente la deuxième activité principale à réaliser par les utilisateurs finaux du système. Cette activité sert principalement à définir les spécifications du système de manière flexible par les administrateurs. De plus, elle donne aux utilisateurs finaux la possibilité de concevoir différentes interfaces graphiques en fonction de leurs préférences et du contexte d'utilisation. La Figure 6.13 montre un diagramme de cas d'utilisation pour la configuration dynamique et la conception personnalisée. Comme nous pouvons le voir dans la Figure 6.13, la configuration dynamique et l'activité de conception personnalisée se compose de deux sous-activités qui sont: (1) configuration des spécifications; et (2) création de templates. La configuration des spécifications est la procédure de configuration de plusieurs paramètres en lien avec l'information en attribuant des valeurs spécifiques à chacun de ces paramètres. Pour simplifier les tâches de l'administrateur dans l'activité de configuration de spécification, il doit être en mesure de configurer ces paramètres en fonction d'un ensemble de valeurs proposées. Par conséquent, nous avons proposé de définir ces valeurs comme des instances de concepts dans la base de connaissances. De plus, chaque valeur doit avoir des fonctions pré-implémentées et intégrées dans le système. La Figure 6.14 illustre un diagramme de séquence pour l'activité de configuration des spécifications. En ce qui concerne la création de templates, cette activité consiste à créer et concevoir différents templates en: (1) Visualisant différents groupes d'informations et d'éléments d'information dans des composants spécifiques en fonction de l'activité de configuration des spécifications; (2) Intégrant les composants multimédias requis dans les templates; et (3) Positionnant différents éléments d'information et composants sur ces templates. Cette étape aboutit à plusieurs templates personnalisés où chaque template est spécifique à l'utilisateur qui le crée et à un contexte d'utilisation spécifique. De plus, chaque template est

A. RÉSUMÉ DE LA THÈSE

adaptable à la taille de l'instrument de communication sélectionné. La Figure 6.17 illustre un diagramme de séquence pour l'activité de création de templates.

A.6.5 Communication et contrôle d'accès

Cette activité consiste à transmettre, recevoir, et visualiser des informations en garantissant un accès confidentiel à ces informations. La Figure 6.20 montre un diagramme de cas d'utilisation pour le système de communication MODES. Comme nous pouvons le voir dans la Figure 6.20, l'activité de communication se compose de quatre sous-activités qui sont: (1) l'authentification de l'utilisateur; (2) Connexion à l'intervention et sélection du contexte; (3) Réception et consultation d'informations; et (4) la transmission d'informations.

A.6.5.1 Authentification et sélection du contexte et d'intervention

Étant donné que la plateforme est basée sur la conception et la mise en œuvre d'un système de communication personnalisé qui garantit la confidentialité de l'information, il est indispensable d'intégrer un mécanisme d'authentification. Dans ce contexte, nous adoptons un mécanisme d'authentification basé sur le JSON Web Token (JWT) [Jones *et al.*, 2015]. La Figure 6.21 illustre un diagramme de séquence pour le mécanisme d'authentification des utilisateurs intégré à la plateforme basé sur JWT. Après s'être authentifié sur la plateforme, créé différents contextes et templates, l'utilisateur final procédera à l'utilisation du système de communication. Dans ce contexte, il faut sélectionner une intervention spécifique à travers un ensemble d'interventions créées. De plus, le contexte d'utilisation doit être sélectionné à travers une liste de contextes créée par l'utilisateur au préalable. Cela permet de récupérer le template créé précédemment et générer une interface graphique correspondante. La Figure 6.22 illustre un diagramme de séquence pour la sélection de l'intervention et du contexte.

A.6.5.2 Contrôle d'accès et gestion des droits

Plusieurs modèles de contrôle d'accès ont été proposés dans la littérature. Ces modèles ont été proposés sur la base d'exigences et d'objectifs distincts. Un de ces modèles est le modèle TT-RBAC. Le modèle TT-RBAC peut être très avantageux pour contrôler les autorisations dans les environnements collaboratifs puisqu'il

prend en compte différents paramètres à considérer. La Figure 6.23 illustre le modèle Core TT-RBAC. Malgré ses avantages dans les environnements collaboratifs, TT-RBAC ne peut pas être complètement adopté dans notre solution. Par conséquent, nous modifions ce modèle et l'adaptions pour mieux répondre aux besoins opérationnels. Ces modifications aboutissent à un modèle TT-RBAC adapté. La figure 6.24 illustre le modèle de contrôle d'accès obtenu basé sur l'adaptation de TT-RBAC. Après avoir modélisé tous les éléments du système et leurs relations, il est nécessaire de proposer le mécanisme de contrôle de l'accès sur la base du modèle proposé. En se basant sur ce modèle, il est essentiel de définir différents droits d'accès. Sur la base de ces droits et de différentes combinaisons, les permissions pour différentes actions peuvent être contrôlées. La Figure 6.25 montre un diagramme de cas d'utilisation pour le contrôle d'accès et la gestion des droits. Comme on peut le voir dans la Figure 6.25, le contrôle d'accès et l'activité de gestion des droits se compose de deux sous-activités: gestion des droits, et le contrôle des permissions. L'activité de gestion des droits précède le contrôle des permissions. Il sert principalement à déterminer les droits d'accès. Pour cela, nous proposons de définir les différents droit d'accès en fonction de différents tâches et rôles des utilisateurs formalisés dans l'ontologie ResOnt. Dans ce contexte, nous avons utilisé les règles SWRL pour déterminer ces droits d'une manière automatique. Le Tableau 6.1 inclut les différentes règles SWRL nécessaires pour déterminer les droits d'accès. Grâce à ces règles, il est possible d'identifier le droit d'accès que possède un rôle de membre d'organisation (r) sur un groupe d'informations (g) sur la base de tâches (t) associées au rôle, de groupes d'informations produits ou utilisés par chaque tâche et la fonctionnalité à laquelle chaque tâche est associée.

En ce qui concerne le contrôle des permissions, ce dernier consiste à contrôler différentes actions sur l'information pendant le fonctionnement du système en se basant sur les droits, les combinaisons entre les différents paramètres, et la politique de contrôle d'accès. Nous proposons de contrôler ces permissions sur la base: (1) des connaissances statiques représentées dans la base de connaissances; (2) Informations dynamiques stockées dans la base de données. Pour cela, nous proposons un algorithme pour déterminer le type d'accès en se basant sur les connaissances statiques et les actions. On note que quatre actions d'utilisateurs sont possibles selon le modèle CRUD qui sont: Create, Read, Update, et Delete. La fonction présentée dans l'algorithme 1 représente la fonction qui sera exécuté

A. RÉSUMÉ DE LA THÈSE

avec chaque action pour déterminer le type d'accès en se basant sur les connaissances statiques. En plus du premier algorithme présenté précédemment, nous proposons trois algorithmes qui servent à assurer un contrôle total des autorisations en fonction des actions des utilisateurs et des informations dynamiques. Le premier algorithme (Algorithme 2) inclut la politique pour l'action *Read*, le second contrôle (Algorithme 3) les permissions en cas de *Delete*, tandis que le troisième (Algorithme 4) sert à autoriser ou interdire les actions *Create* et *Update*.

A.6.5.3 Réception et transmission d'information

La transmission d'informations est une activité principale de communication à réaliser par les utilisateurs finaux. Deux actions principales peuvent être réalisées par l'utilisateur dans ce contexte qui sont: Supprimer ou Créer et transmettre. Afin de simplifier les tâches de l'utilisateur, nous proposons de permettre à l'utilisateur de transmettre ou supprimer les groupes d'informations requis tels que présentés dans le modèle d'interaction au lieu de transmettre chaque élément d'information séparément. La Figure 6.30 montre un diagramme de séquence pour la transmission d'informations en respectant la politique du contrôle d'accès. Concernant la réception et de consultation d'informations, cette activité est basée sur l'extraction des valeurs d'informations d'un certain groupe d'informations à partir de la base de données en respectant la politique du contrôle d'accès. En conséquence, il correspond à l'action de lecture et suit principalement l'activité de transmission d'informations. La Figure 6.29 montre un diagramme de séquence pour la réception et la consultation d'informations.

A.7 Expérimentations

Afin de montrer la pertinence de nos hypothèses, nous avons développé la plateforme conçue sur la base des spécifications décrites dans la section A.6. De plus, les différentes fonctionnalités décrites dans la section A.6 ont été développées et intégrées dans la plateforme. Après avoir développé la plateforme proposée, il est nécessaire de la tester afin de l'évaluer. Dans cette thèse, nous n'avons pas eu l'occasion de tester la plate-forme développée par ses utilisateurs finaux. En conséquence, nous proposons de le tester par nous-mêmes afin de valider les fonctionnalités implémentées. Pour cela nous avons configuré les spécifications du système. De plus, nous avons créé différents contextes pour plusieurs utilisateurs. Ensuite, nous avons conçu un template par contexte. Une description

détaillée sur ce test est présentée dans la section 7.3. Les résultats obtenus montrent l'efficacité de la plateforme développée pour configurer les spécifications du système et concevoir des interfaces personnalisées de manière flexible. Cette plateforme a été testée aussi pour évaluer les différentes fonctionnalités liées à la communication. Pour cela, nous avons décrit un scénario fictif d'incident de la route. Ce scénario est décrit en détail dans la section 7.4.1. De plus, nous avons testé la création, transmission, et réception des groupes d'informations. Ce test est présenté dans la section 7.4.2. On note que, vu qu'elle est en sa première version, cette plateforme a différentes limites. Premièrement, cette plateforme n'inclut pas d'interface pour créer une intervention, affecter différentes équipes à une intervention et affecter des membres à ces équipes. Deuxièmement, dans cette plateforme, il n'est pas possible de sélectionner le destinataire de chaque information. Chaque information transmise est automatiquement reçue par tous les acteurs qui ont le droit d'accéder à ces informations. Cependant, le destinataire de chaque message doit être pris en considération. Troisièmement, concernant spécifications liées à l'information, seules les fonctions requises liées au composant d'interface et au type de champ sont considérées parmi les différentes propriétés. Cependant, d'autres propriétés représentées par le type de données de chaque information, le degré de sa criticité, l'orientation et la catégorie doivent être prises en compte. Quatrièmement, en ce qui concerne les composants d'interfaces, il est essentiel de faire la différence entre les composants d'interface d'entrée et de sortie. Cinquièmement, en ce qui concerne les composants multimédias, les utilisateurs finaux peuvent intégrer des composants multimédias de sortie dans leurs interfaces. Cependant, l'intégration des composants multimédias d'entrée et des différentes fonctions liées à la transmission et à la réception multimédias ne sont pas prises en compte dans la plateforme. Sixièmement, dans la version actuelle de la plateforme, chaque utilisateur doit sélectionner son contexte dans l'intervention afin de récupérer l'interface correspondante. Lorsqu'un utilisateur doit modifier son contexte, l'utilisateur doit le modifier manuellement. Cependant, dans les pratiques réelles, les utilisateurs n'ont pas le temps de changer de contexte lors d'une intervention. Le passage d'un contexte utilisateur à un autre contexte doit être géré automatiquement. Septièmement, certains groupes d'informations ont des cas particuliers. Ces groupes sont généralement indépendants des interventions. Par conséquent, ils diffèrent des autres groupes en termes de conception et de consultation. Le cas particulier de ces groupes n'est pas pris en compte dans cette plateforme. Enfin, dans ce travail, nous n'avons pas eu l'occasion de

tester la plateforme par ses utilisateurs finaux. Cela devrait être amélioré pour un véritable système utilisable par les acteurs du secours.

A.8 Conclusions et perspectives

A.8.1 Conclusion générale

Cette thèse a abordé le problème de conscience mutuelle dans un environnement collaboratif: Le secours à personne. Nous nous sommes basés sur la proposition d'une solution de support à la communication pour garantir une conscience mutuelle entre les différents acteurs. Dans ce contexte, nous avons proposé une approche pour concevoir un système personnalisé pour supporter la conscience et la communication dans les opérations de secours qui garantit la confidentialité des informations.

La première étape consiste à examiner et modéliser les interactions à partir de pratiques réelles. L'importance de cette étape est d'identifier les informations requises par chaque personne en fonction de son rôle, de son contexte et des tâches à accomplir. En conséquence, nous avons analysé différentes interactions dans les opérations de secours sur la base d'une étude approfondie des documents, rapports et législations liés au domaine.

La deuxième étape repose sur la construction d'une ontologie d'application qui représente les connaissances nécessaires à la conception d'un système de communication orienté vers les acteurs du secours qui garantit la confidentialité de l'information. Pour cela, nous avons développé une ontologie d'application appelée ResOnt.

La troisième étape consiste à développer une plateforme basée sur l'ontologie pour la conception et la communication. Cette plateforme permettra aux utilisateurs finaux de définir les spécifications du système et de concevoir ses interfaces de manière personnalisée. En conséquence, nous avons présenté une plateforme de conception et de communication basée sur le modèle d'interaction et l'ontologie ResOnt.

La quatrième étape repose sur l'intégration des mécanismes de confidentialité dans le système. Dans cette thèse, nous nous sommes concentrés sur le mécanisme de contrôle d'accès. Dans ce cadre, nous avons proposé une politique de contrôle

d'accès et de gestion des droits pour garantir l'accès confidentiel aux informations de la plateforme. Pour cela, nous avons adapté et modifié le modèle TT-RBAC et proposé un nouveau modèle de contrôle d'accès.

La cinquième étape consiste à concevoir les spécifications et les interfaces du système par ses utilisateurs finaux de manière personnalisée via la plateforme proposée. Ainsi, nous avons implémenté un premier prototype de la plateforme. De plus, nous avons développé et intégré différentes fonctions et mécanismes requis dans la plateforme développée. De plus, nous avons réalisé plusieurs expériences liées à la conception et à la communication en utilisant la plateforme développée afin de la tester.

A.8.2 Perspectives

Dans le cadre de travaux futurs, nous tenons à étudier les aspects suivants concernant l'amélioration des méthodes proposées.

- *Extension du modèle d'interaction proposé* : Pour analyser et modéliser différentes interactions, nous avons adopté une approche basée sur une description de scénario. Dans ce contexte, nous avons décrit un scénario d'une opération de secours en France à la suite d'un incident qui affecte plusieurs victimes. Dans ce scénario, seuls deux services ont été considérés: les pompiers et les services médicaux. Cependant, dans des scénarios réels, d'autres services peuvent être impliqués comme la police. En conséquence, ce modèle devrait être généralisé pour couvrir différents scénarios possibles. Dans ce contexte, différents types d'incidents et de services doivent être considérés.
- *Validation du modèle d'interaction proposé* : Pour des raisons de temps et de confidentialité, nous n'avons pas pu accéder au terrain afin d'analyser les pratiques réelles des acteurs du secours. De plus, bien que ce modèle soit basé sur une étude approfondie de la documentation liée au domaine, nous n'avons pas pu rencontrer des experts du domaine pour le valider. Par conséquent, nous proposons de valider ce modèle avec une étude de cas réel afin de l'évaluer par des experts du domaine.
- *Compléter l'ontologie ResOnt* : Plusieurs concepts liés à la conception des systèmes et des interfaces n'ont pas été définis dans ResOnt. De plus, d'autres aspects liés aux communications tels que les infrastructures et les

A. RÉSUMÉ DE LA THÈSE

réseaux n'ont pas été pris en compte dans ResOnt. Par ailleurs, concernant la confidentialité de l'information, puisque ces travaux portent sur les mécanismes de contrôle d'accès, la définition des concepts dans ResOnt s'est limitée aux concepts liés à ce mécanisme. Dans ce contexte, nous proposons de compléter l'ontologie ResOnt afin de couvrir différents aspects liés à la conception, à la communication et à la confidentialité de l'information.

- *Évaluation de l'ontologie ResOnt par des experts du domaine* : Il existe plusieurs approches pour l'évaluation d'ontologie. Dans cette thèse, nous avons adopté l'approche applicative pour évaluer l'ontologie ResOnt. Cependant, l'approche basée sur l'utilisateur permet une évaluation meilleure et plus complète par rapport aux autres approches. Par conséquent, une évaluation de l'ontologie ResOnt par des experts du domaine est proposée dans travail futur. Suite à cette évaluation, nous enrichirons cette ontologie en fonction des besoins et des suggestions.
- *Implémentation d'une plateforme complète intégrant différentes fonctionnalités* : Dans cette thèse, le travail d'implémentation s'est limité au développement d'une plateforme locale permettant la conception d'interfaces ainsi que l'échange local d'informations. En tant que travail futur, cette plateforme doit être étendue en un système complet qui comprend les différentes fonctionnalités et mécanismes requis. De plus, plusieurs améliorations sur les fonctionnalités développées dans la version actuelle doivent être effectuées.
- *Évaluation de la plateforme développée par les utilisateurs finaux* : La plateforme développée doit être testée et évaluée par ses utilisateurs finaux. En conséquence, nous proposons de fournir cette plateforme aux services impliqués dans les opérations de secours afin de la tester dans des scénarios réels. Plusieurs modifications peuvent alors être effectuées sur la plateforme en fonction des besoins, des exigences et des suggestions des utilisateurs finaux.

En ce qui concerne les perspectives à long terme, nous cherchons à :

- *Rendre l'ontologie ResOnt accessible au public* : Puisque l'ontologie ResOnt n'est pas évaluée par les experts du domaine, nous ne l'avons pas rendue accessible au public. Par conséquent, suite à son évaluation, nous proposons de le soumettre et de le publier dans un catalogue d'ontologie.

- *Application de l'approche proposée à d'autres environnements* : Dans cette thèse, l'application de l'approche proposée se limitait au domaine des opérations de secours. Nous proposons d'étudier l'application de cette approche dans d'autres environnements collaboratifs pour valider sa pertinence.

A. RÉSUMÉ DE LA THÈSE

Bibliography

- ABOMHARA, M., YANG, H. & KØIEN, G.M. (2016). Access control model for cooperative healthcare environments: Modeling and verification. In *2016 IEEE International Conference on Healthcare Informatics (ICHI), USA*, 46–54, IEEE. [163](#), [290](#)
- ABOU EL KALAM, A., EL BAIDA, R., BALBIANI, P., BENFERHAT, S., CUPPENS, F., DESWARTE, Y., MIEGE, A., SAUREL, C. & TROUESSIN, G. (2003). Or-bac: un modèle de contrôle d'accès basé sur les organisations. *Cahiers francophones de la recherche en sécurité de l'information. II*, **43**, 30–43. [84](#)
- ABOWD, G.D., DEY, A.K., BROWN, P.J., DAVIES, N., SMITH, M. & STEGGLES, P. (1999). Towards a better understanding of context and context-awareness. In *International symposium on handheld and ubiquitous computing, Germany*, 304–307, Springer. [27](#)
- ACKOFF, R. (1997). Transformational consulting. *Management Consulting Times*, **28**, 1997. [56](#)
- AL-BALTAH, I.A., GHANI, A.A.A., RAHMAN, W.N.W.A. & ATAN, R. (2014). A comparative study on ontology development methodologies towards building semantic conflicts detection ontology for heterogeneous web services. *Research Journal of Applied Sciences, Engineering and Technology*, **7**, 2674–2679. [125](#)
- ALEXANDRE, B., REYNAUD, E., OSIURAK, F. & NAVARRO, J. (2018). Acceptance and acceptability criteria: a literature review. *Cognition, Technology & Work*, **20**, 165–177. [10](#), [263](#)

BIBLIOGRAPHY

- ALI, M.M., RAI, R., OTTE, J.N. & SMITH, B. (2019). A product life cycle ontology for additive manufacturing. *Computers in Industry*, **105**, 191–203. [134](#)
- ANDERSON, A., NADALIN, A., PARDUCCI, B., ENGOVATOV, D., LOCKHART, H., KUDO, M., HUMENN, P., GODIK, S., ANDERSON, S., CROCKER, S. *et al.* (2003). Extensible access control markup language (xacml) version 1.0. *OASIS*. [82](#)
- ARP, R., SMITH, B. & SPEAR, A.D. (2015). *Building ontologies with basic formal ontology*. MIT Press. [64](#), [71](#), [133](#), [134](#)
- ARTMAN, H. & GARBIS, C. (1998). Situation awareness as distributed cognition. In *Proceedings of the 9th European Conference on Cognitive Ergonomics*, vol. 98, Citeseer. [24](#)
- ASUNCIÃO, G.P., MARIANO, F.L. & OSCAR, C. (2004). *Ontological engineering: with examples from the areas of knowledge management, e-commerce and the semantic Web*. Springer-Verlag, London New York. [64](#)
- ATIFI, H. (2016). Communication, cmc and e-mail: A brief survey. *Daily Knowledge Valuation in Organizations: Traceability and Capitalization*, 123–151. [29](#)
- BACHIMONT, B. (2004). Pourquoi n’y a-t-il pas d’expérience en ingénierie des connaissances ? In *Proceedings of Ingénierie des connaissances (IC 2004)*, France, 1–12. [55](#)
- BANNOUR, W., MAALEL, A. & GHEZALA, H.H.B. (2019). Ontology-based representation of crisis response situations. In *International Conference on Computational Collective Intelligence, France*, 417–427, Springer. [73](#), [75](#)
- BARROS, R., KISLANSKY, P., DO NASCIMENTO SALVADOR, L., ALMEIDA, R., BREYER, M. & PEDRAZA, L.G. (2015). Edxl-rescuer ontology: Conceptual model for semantic integration. In *Proceedings of the 12th International Conference on Information Systems for Crisis Response and Management (IS-CRAM)*, Norway. [66](#), [71](#), [74](#)
- BARTHEL, B.A. (2012). 9/11 ten years after: Command, control, communications remain an issue. Tech. rep., United States Army War College. [7](#)

- BECHHOFFER, S., VAN HARMELEN, F., HENDLER, J., HORROCKS, I., MCGUINNESS, D.L., PATEL-SCHNEIDER, P.F. & STEIN, L.A. (2004). Owl web ontology language reference. *W3C recommendation*, **10**. [67](#)
- BEDNY, G. & MEISTER, D. (1999). Theory of activity and situation awareness. *International Journal of cognitive ergonomics*, **3**, 63–72. [18](#), [22](#), [23](#), [24](#)
- BELKADI, F., BONJOUR, E., CAMARGO, M., TROUSSIER, N. & EYNARD, B. (2013). A situation model to support awareness in collaborative design. *International Journal of Human-Computer Studies*, **71**, 110–129. [18](#), [19](#), [20](#), [21](#)
- BELL, D.E. & LA PADULA, L.J. (1976). Secure computer system: Unified exposition and multics interpretation. Tech. rep., MITRE CORP BEDFORD MA. [192](#)
- BÉNABEN, F., HANACHI, C., LAURAS, M., COUJET, P. & CHAPURLAT, V. (2008). A metamodel and its ontology to guide crisis characterization and its collaborative management. In *Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management (ISCRAM), USA*, 4–7. [41](#), [42](#), [72](#), [75](#)
- BÉNABEN, F., LAURAS, M., TRUPTIL, S. & SALATGÉ, N. (2016). A meta-model for knowledge management in crisis management. In *2016 49th Hawaii International Conference on System Sciences (HICSS), USA*, 126–135, IEEE. [72](#)
- BENJAMINS, R., FENSEL, D., STRAATMAN, R. *et al.* (1996). Assumptions of problem-solving methods and their role in knowledge engineering. In *Proceedings of the 12th European Conference on Artificial Intelligence, Hungary*, 408–412, PITMAN. [65](#)
- BERNERS-LEE, T., HENDLER, J. & LASSILA, O. (2001). The semantic web. *Scientific american*, **284**, 34–43. [60](#)
- BERTRAND, M. (2018). Secours d’urgence aux personnes (SUAP) : l’état des lieux de la bspp. Retrieved from <https://allo18-lemag.fr/service-durgence-aux-personnes-suap-letat-des-lieux/> (accessed 01 January 2021). [6](#)

BIBLIOGRAPHY

- BEZERRA, C., FREITAS, F. & SANTANA, F. (2013). Evaluating ontologies with competency questions. In *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, vol. 3, 284–285. [128](#), [281](#)
- BLÁZQUEZ, L.M.V., POVEDA, M.Á.B., SUÁREZ-FIGUEROA, M.C., GÓMEZ-PÉREZ, A. & PASCUAL, A.F.R. (2007). Towntology & hydrontology: Relationship between urban and hydrographic features in the geographic information domain. In *Ontologies for Urban Development*, 73–84, Springer. [65](#), [136](#)
- BONATTI, A., DE COI, J., SAURO, L. & OLMEDILLA, D. (2008). Protune: a framework for semantic web policies. In *Proceedings of the Poster and Demonstration Session at the 7th International Semantic Web Conference (ISWC2008), Germany*, Citeseer. [82](#)
- BONTCHEVA, K. & WILKS, Y. (2004). Automatic report generation from ontologies: the miakt approach. In *International conference on application of natural language to information systems, United Kingdom*, 324–335, Springer. [76](#)
- BORST, P., AKKERMANS, H. & TOP, J. (1997). Engineering ontologies. *International journal of human-computer studies*, **46**, 365–406. [61](#), [62](#)
- BRACHMAN, R.J. & LEVESQUE, H.J. (1986). Knowledge representation and reasoning. *Annual review of computer science*, **1**, 255–287. [57](#), [58](#)
- BRACHMAN, R.J., MCGUINNESS, D.L., PATEL-SCHNEIDER, P.F., RESNICK, L.A. & BORGIDA, A. (1991). Living with classic: When and how to use a KL-ONE-like language. In *Principles of semantic networks*, chap. 14, 401–456, Elsevier. [59](#)
- BRANK, J., GROBELNIK, M. & MLADENIC, D. (2005). A survey of ontology evaluation techniques. In *Proceedings of the conference on data mining and data warehouses (SiKDD 2005), Slovenia*, 166–170. [141](#), [283](#)
- BRAY, T., PAOLI, J., SPERBERG-MCQUEEN, C.M., MALER, E. & YERGEAU, F. (1997). Extensible markup language (xml). *World Wide Web Journal*, **2**, 27–66. [67](#)

- BUFFA, M. & FARON-ZUCKER, C. (2012). Ontology-based access rights management. In *Advances in Knowledge Discovery and Management*, 49–61, Springer. [83](#), [85](#), [149](#)
- BUNKER, D., LEVINE, L. & WOODY, C. (2015). Repertoires of collaboration for common operating pictures of disasters and extreme events. *Information Systems Frontiers*, **17**, 51–65. [31](#)
- CARR, L., HALL, W., BECHHOFFER, S. & GOBLE, C. (2001). Conceptual linking: ontology-based open hypermedia. In *Proceedings of the 10th international conference on World Wide Web, Hong Kong*, 334–342. [76](#)
- CARROLL, J.M., ROSSON, M.B., CONVERTINO, G. & GANOE, C.H. (2006). Awareness and teamwork in computer-supported collaborations. *Interacting with computers*, **18**, 21–46. [19](#)
- CARVER, L. & TUROFF, M. (2007). Human-computer interaction: the human and computer as a team in emergency management information systems. *Communications of the ACM*, **50**, 33–38. [41](#)
- CASADO, R., RUBIERA, E., SACRISTAN, M., SCHÜTTE, F. & PETERS, R. (2015). Data interoperability software solution for emergency reaction in the europe union. *Natural Hazards & Earth System Sciences*, **15**. [66](#), [71](#), [74](#)
- CASTELLS, P. & MACÍAS, J.A. (2001). An adaptive hypermedia presentation modeling system for custom knowledge representations. In *Proceedings of Web-Net 2001 - World Conference on the WWW and Internet, USA*, 148–153. [79](#)
- CASTILLEJO, E., ALMEIDA, A. & LÓPEZ-DE IPIÑA, D. (2014). Ontology-based model for supporting dynamic and adaptive user interfaces. *International Journal of Human-Computer Interaction*, **30**, 771–786. [78](#), [81](#)
- CAZENEUVE, B. & TOURAINÉ, M. (2015). “Circulaire interministérielle DGOS/R2/DGSCGC no 2015-190 du 5 juin 2015 relative à l’application de l’arrêté du 24 avril 2009 relatif à la mise en oeuvre du référentiel portant sur l’organisation du secours à personne et de l’aide médicale urgente”. *BO Santé – Protection sociale – Solidarité*, no **2015/7**, 10. [91](#)
- CHAAWA, M., THABET, I., HANACHI, C. & BEN SAID, L. (2017). Modelling and simulating a crisis management system: an organisational perspective. *Enterprise Information Systems*, **11**, 534–550. [36](#), [37](#)

BIBLIOGRAPHY

- CHAN, J.L. & PUROHIT, H. (2019). Challenges to transforming unconventional social media data into actionable knowledge for public health systems during disasters. *Disaster medicine and public health preparedness*. 7
- CHAN, S., HAUGH, B., LOAIZA-LEMONS, F. & WARTIK, S. (2017). Public safety and emergency management communications ontology. *IDA Document D-8583*, 1. 72, 74
- CHANDRASEKARAN, B., JOSEPHSON, J.R. & BENJAMINS, V.R. (1999). What are ontologies, and why do we need them? *IEEE Intelligent Systems and their applications*, 14, 20–26. 59, 60, 62, 63
- CHANNA, M.I. & AHMED, K.M. (2010). Emergency response communications and associated security challenges. *International Journal of Network Security and Its Applications (IJNSA)*, 2. 42
- CHEAITO, M. (2012). *Un cadre de spécification et de déploiement de politiques d'autorisation*. Ph.D. thesis, Université Toulouse III-Paul Sabatier, France. 81, 272
- CHOO, C.W., DETLOR, B. & TURNBULL, D. (2013). *Web work: Information seeking and knowledge work on the World Wide Web*, vol. 1. Springer Science & Business Media. 56
- CIRIO, L., CRUZ, I.F. & TAMASSIA, R. (2007). A role and attribute based access control system using semantic web technologies. In *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*, Portugal, 1256–1266, Springer. 83, 85
- CLARK, H.H. & BRENNAN, S.E. (1991). Grounding in communication. *Readings in Groupware and Computer Supported Cooperative Work: Assisting Human-Human Collaboration*, 127–149. 27
- COCHE, J., MONTARNAL, A., TAPIA, A. & BENABEN, F. (2019). Actionable collaborative common operational picture in crisis situation: A comprehensive architecture powered with social media data. In *Working Conference on Virtual Enterprises*, 151–162, Springer. 9, 41
- COMFORT, L.K., KO, K. & ZAGORECKI, A. (2004). Coordination in rapidly evolving disaster response systems: The role of information. *American behavioral scientist*, 48, 295–313. 5

- CONVERTINO, G., NEALE, D.C., HOBBY, L., CARROLL, J.M. & ROSSON, M.B. (2004). A laboratory method for studying activity awareness. In *Proceedings of the third Nordic conference on Human-computer interaction, USA*, 313–322. [19](#)
- CORCHO, O., FERNÁNDEZ-LÓPEZ, M. & GÓMEZ-PÉREZ, A. (2003). Methodologies, tools and languages for building ontologies. where is their meeting point? *Data & knowledge engineering*, **46**, 41–64. [125](#), [127](#), [270](#), [280](#)
- CORCHO, O., GÓMEZ-PÉREZ, A. & FERNÁNDEZ-LÓPEZ, M. (2004). Ontological engineering. *Advanced Information and Knowledge Processing*, **1**. [125](#)
- CORCHO, O., FERNÁNDEZ-LÓPEZ, M., GÓMEZ-PÉREZ, A. & LÓPEZ-CIMA, A. (2005). Building legal ontologies with methontology and webode. In *Law and the semantic web*, 142–157, Springer. [142](#), [284](#)
- CORCHO, O., FERNÁNDEZ-LÓPEZ, M. & GÓMEZ-PÉREZ, A. (2006). Ontological engineering: principles, methods, tools and languages. In *Ontologies for software engineering and software technology*, 1–48, Springer. [68](#), [270](#)
- CRAIG, R.T. (2006). Communication as a practice. *Communication as a practice: Perspectives on theory*, 38–48. [29](#)
- CRISTANI, M. & CUEL, R. (2005). A survey on ontology creation methodologies. *International Journal on Semantic Web and Information Systems (IJSWIS)*, **1**, 49–69. [68](#)
- CRYSTAL, D. (2004). *The Cambridge encyclopedia of the English language*. Ernst Klett Sprachen. [2](#)
- DAMIANOU, N., DULAY, N., LUPU, E. & SLOMAN, M. (2001). The ponder policy specification language. In *International Workshop on Policies for Distributed Systems and Networks, UK*, 18–38, Springer. [82](#)
- DAVENPORT, T.H. & PRUSAK, L. (1997). *Information ecology: Mastering the information and knowledge environment*. Oxford University Press on Demand. [56](#)
- DAVENPORT, T.H. & PRUSAK, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press. [56](#)

BIBLIOGRAPHY

- DÉCUGIS, J.M. & PELLETIER, E. (2018). Après la mort d'un soldat du feu, la lettre d'indignation du patron des pompiers de paris. Retrieved from <http://www.leparisien.fr/faits-divers/la-lettre-d-indignation-du-patron-des-pompiers-de-paris-12-09-2018-7886160.php> (accessed 30 July 2019). [3](#)
- DE GAULLE, J. (1839). *Nouvelle histoire de Paris et de ses environs*. Pourrat. [4](#)
- DE NICOLA, A., MISSIKOFF, M. & NAVIGLI, R. (2009). A software engineering approach to ontology building. *Information systems*, **34**, 258–275. [69](#), [125](#)
- DE OLIVEIRA, R.F., DAMISCH, L., HOSSNER, E.J., OUDEJANS, R.R., RAAB, M., VOLZ, K.G. & WILLIAMS, A.M. (2009). The bidirectional links between decision making, perception, and action. *Progress in brain research*, **174**, 85–93. [9](#), [250](#)
- DERBALE, A. & MEHENNI, O. (2003). *Sécurisation du dossier médical à base d'ontologie*. Master's thesis, University of Abou Bakr Belkaidde Tlemcen, Algeria. [84](#), [85](#)
- DÉTIENNE, F. (2006). Collaborative design: Managing task interdependencies and multiple perspectives. *Interacting with computers*, **18**, 1–20. [21](#)
- DETTBORN, T., KÖNIG-RIES, B. & WELSCH, M. (2008). Using semantics in portal development. In *Proceedings of the 4th International Workshop on Semantic Web Enabled Software Engineering, USA*, 109–110. [76](#)
- DIEDERICHS, O., PAULOT, J.M., MAUSS, H. & MAYMIL, V. (2006). Rescue of people, secours à personne. *Rapport de l'Inspection générale de l'administration*. [2](#), [274](#)
- DIX, A., DIX, A.J., FINLAY, J., ABOWD, G.D. & BEALE, R. (2003). *Human-computer interaction, Second Edition*. Pearson Education. [26](#)
- DOURISH, P. & BELLOTTI, V. (1992). Awareness and coordination in shared workspaces. In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work, Canada*, 107–114. [18](#), [19](#)
- DÖWELING, S., PROBST, F., ZIEGERT, T. & MANSKE, K. (2009). Soknos—an interactive visual emergency management framework. In *GeoSpatial Visual Analytics*, chap. 20, 251–262, Springer. [41](#)

- DOWNES, D.D., RUB, J.R., KUNG, K.C. & JORDAN, C.S. (1985). Issues in discretionary access control. In *1985 IEEE Symposium on Security and Privacy, USA*, 208–208, IEEE. [192](#)
- DUMONTIER, M. & HOEHNDORF, R. (2010). Realism for scientific ontologies. In *The 6th International Conference on Formal Ontology in Information Systems, Canada*, 387–399. [135](#), [282](#)
- EHRlich, K. & CHANG, K. (2006). Leveraging expertise in global software teams: Going outside boundaries. In *2006 IEEE International Conference on Global Software Engineering (ICGSE), Brazil*, 149–158, IEEE. [19](#)
- EL KALAM, A.A. (2003). *Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales*. Ph.D. thesis, Laboratoire d'Analyse et d'Architecture des Systèmes du Centre National de la Recherche Scientifique, France. [10](#)
- ELMASLLARI, E. (2019). Design and development methods for improving acceptance of it among emergency responders. In *Proceedings of the 16th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Spain*, 1300–1309. [7](#), [161](#), [261](#)
- ELMHADHBI, L. (2020). *Ontology-driven services for interoperable multi-stakeholders operational disaster response*. Ph.D. thesis, Institut National Polytechnique de Toulouse, France. [5](#), [6](#), [39](#), [47](#), [49](#), [50](#), [75](#), [90](#), [117](#), [133](#), [138](#), [215](#), [216](#)
- ELMHADHBI, L., KARRAY, M.H. & ARCHIMÈDE, B. (2018). An ontology-based emergency response system for interoperability in a crisis situation in smart cities. *Enterprise Interoperability: Smart Services and Business Impact of Enterprise Interoperability VIII*, 421–427. [135](#)
- ELMHADHBI, L., KARRAY, M.H. & ARCHIMÈDE, B. (2019). A modular ontology for semantically enhanced interoperability in operational disaster response. In *Proceedings of the 16th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Spain*, 1021–1029. [71](#), [74](#), [133](#), [134](#), [136](#), [147](#), [282](#)
- ENDSLEY, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, **37**, 32–64. [18](#), [21](#), [22](#), [23](#), [24](#), [25](#), [28](#)

BIBLIOGRAPHY

- ENDSLEY, M.R. (2006). Situation awareness. *Handbook of human factors and ergonomics*, **3**, 528–542. [21](#), [26](#)
- ENDSLEY, M.R. (2016). *Designing for situation awareness: An approach to user-centered design, Second Edition*. CRC press, Taylor & Francis Group. [22](#)
- ENDSLEY, M.R. & ROBERTSON, M.M. (1996). Team situation awareness in aviation maintenance. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, USA*, 1077–1081. [27](#)
- FABRIKANT, S.I. (2001). Building task-ontologies for geovisualization. In *Pre-Conference Workshop on Geovisualization on the Web, China*. [65](#)
- FALQUET, G., MÉTRAL, C., TELLER, J. & TWEED, C. (2011). *Ontologies in urban development projects*. Springer Science & Business Media. [64](#), [68](#), [269](#)
- FAN, Z. & ZLATANOVA, S. (2011). Exploring ontologies for semantic interoperability of data in emergency response. *Applied Geomatics*, **3**, 109–122. [73](#), [75](#)
- FEDOSEJEV, A. (2015). *React.js essentials*. Packt Publishing Ltd. [166](#)
- FENECH, G. & PIETRASANTA, S. (2016). Rapport fait au nom de la commission d'enquête relative aux moyens mis en œuvre par l'état pour lutter contre le terrorisme depuis le 7 janvier 2015, no, 3922. *Assemblée Nationale*, **145**. [3](#), [5](#)
- FENG, M., LI, A., JIA, C. & LIU, Z. (2016). Unconventional emergencies management based on domain knowledge. *Procedia computer science*, **91**, 268–275. [70](#)
- FENSEL, D. (2001). Ontologies. In *Ontologies*, 11–18, Springer. [59](#)
- FERNÁNDEZ-LÓPEZ, M., GÓMEZ-PÉREZ, A. & JURISTO, N. (1997). Methontology: from ontological art towards ontological engineering. In *AAAI Symposium on Ontological Engineering, USA*, 33–40. [68](#), [71](#), [127](#), [128](#), [132](#), [133](#), [138](#), [139](#), [280](#), [282](#), [283](#)
- FININ, T., JOSHI, A., KAGAL, L., NIU, J., SANDHU, R., WINSBOROUGH, W. & THURASINGHAM, B. (2008a). ROWL BAC: representing role based access control in OWL. In *Proceedings of the 13th ACM symposium on Access control models and technologies, USA*, 73–82. [81](#), [82](#), [85](#)

- FININ, T., JOSHI, A., KAGAL, L., NIU, J., SANDHU, R., WINSBOROUGH, W.H. & THURAISSINGHAM, B. (2008b). Role based access control and owl. In *Proceedings of the fourth OWLED Workshop on OWL: Experiences and Directions, USA*, 1–12. [82](#)
- FIGORE, S.M., SALAS, E., CUEVAS, H.M. & BOWERS, C.A. (2003). Distributed coordination space: toward a theory of distributed team process and performance. *Theoretical Issues in Ergonomics Science*, **4**, 340–364. [19](#)
- FLUIT, C., SABOU, M. & VAN HARMELEN, F. (2003). Supporting user tasks through visualisation of light-weight ontologies. In *Handbook on Ontologies in Information Systems*, Citeseer. [76](#)
- FONSECA, F.T., EGENHOFER, M.J., DAVIS JR, C.A. & BORGES, K.A. (2000). Ontologies and knowledge sharing in urban gis. *Computers, Environment and Urban Systems*, **24**, 251–272. [65](#)
- FRENCH MINISTRY OF INTERIOR (2019). Les statistiques des services d’incendie et de secours édition 2019. Retrieved from <https://www.interieur.gouv.fr/Publications/Statistiques/Securite-civile/2018> (accessed 01 May 2020). [3](#), [92](#)
- FRONTINI, F., DEL GRATTA, R. & MONACHINI, M. (2013). Geodomainwordnet: Linking the geonames ontology to wordnet. In *The 6th Language and Technology Conference, Poland*, 229–242, Springer. [136](#)
- FURTADO, E., FURTADO, J.J.V., SILVA, W.B., RODRIGUES, D.T., TADDEO, L.D.S., LIMBOURG, Q. & VANDERDONCKT, J. (2001). An ontology-based method for universal design of user interfaces. In *Proceedings of Workshop on Multiple User Interfaces over the Internet: Engineering and Applications Trends MUI, France*, 1–9. [77](#), [81](#), [147](#)
- GANGEMI, A., GUARINO, N., MASOLO, C., OLTRAMARI, A. & SCHNEIDER, L. (2002). Sweetening ontologies with dolce. In *International Conference on Knowledge Engineering and Knowledge Management, Spain*, 166–181, Springer. [64](#), [71](#), [76](#), [134](#)
- GIERE, R.N. (2004). How models are used to represent reality. *Philosophy of science*, **71**, 742–752. [90](#)

BIBLIOGRAPHY

- GLAA, B. (2008). *Contribution à la conception et l'optimisation d'un système d'aide à la gestion des urgences*. Ph.D. thesis, Ecole Centrale de Lille, France. [4](#)
- GLASSEY, O. (2008). A case study on process modelling—three questions and three techniques. *Decision Support Systems*, **44**, 842–853. [103](#), [278](#)
- GÓMEZ-PÉREZ, A. & CORCHO, O. (2002). Ontology languages for the semantic web. *IEEE Intelligent systems*, **17**, 54–60. [67](#)
- GRENON, P., SMITH, B. & GOLDBERG, L. (2004). Biodynamic ontology: applying bfo in the biomedical domain. *Studies in health technology and informatics*, 20–38. [65](#)
- GRIFFIN, E. (2006). *A first look at communication theory, Second Edition*. New York: McGraw-hill. [29](#)
- GRIMM, S. (2009). Knowledge representation and ontologies. In *Scientific Data Mining and Knowledge Discovery*, chap. 3, 111–137, Springer. [58](#), [59](#), [67](#)
- GROSS, T., STARY, C. & TOTTER, A. (2005). User-centered awareness in computer-supported cooperative work-systems: Structured embedding of findings from social sciences. *International Journal of Human-Computer Interaction*, **18**, 323–360. [19](#), [20](#)
- GRUBER, T.R. (1995). Toward principles for the design of ontologies used for knowledge sharing? *International journal of human-computer studies*, **43**, 907–928. [62](#)
- GRUBER, T.R. *et al.* (1993). A translation approach to portable ontology specifications. *Knowledge acquisition*, **5**, 199–221. [9](#), [59](#), [61](#), [263](#)
- GUARINO, N. (1998). Formal ontology in information systems. In *Proceedings of the First International Conference on Formal Ontology in Information Systems (FOIS 98)*, Italy, vol. 46, IOS press. [64](#)
- GUARINO, N., OBERLE, D. & STAAB, S. (2009). What is an ontology? In *Handbook on ontologies*, 1–17, Springer. [61](#), [62](#)
- GUTWIN, C. & GREENBERG, S. (1995a). Support for group awareness in real-time desktop conferences. In *Proceedings of The Second New Zealand Computer Science Research Students' Conference, New Zealand*, 102–114. [20](#)

- GUTWIN, C. & GREENBERG, S. (1995b). *Workspace awareness in real-time distributed groupware*. Ph.D. thesis, The University of Calgary, Canada. [19](#), [20](#)
- GUTWIN, C. & GREENBERG, S. (2002). A descriptive framework of workspace awareness for real-time groupware. *Computer Supported Cooperative Work (CSCW)*, **11**, 411–446. [19](#), [26](#), [27](#)
- GUTWIN, C., GREENBERG, S. & ROSEMAN, M. (1996a). Supporting awareness of others in groupware. In *Conference Companion on Human Factors in Computing Systems, Canada*, 205–206. [21](#)
- GUTWIN, C., GREENBERG, S. & ROSEMAN, M. (1996b). Workspace awareness in real-time distributed groupware: Framework, widgets, and evaluation. In *People and Computers XI*, 281–298, Springer. [20](#)
- HARRIS, S., SEABORNE, A. & PRUD’HOMMEAUX, E. (2013). Sparql 1.1 query language. *W3C recommendation*, **21**, 778. [164](#), [221](#)
- HERNANDEZ, J.Z. & SERRANO, J.M. (2001). Knowledge-based models for emergency management systems. *Expert systems with applications*, **20**, 173–186. [70](#)
- HLOMANI, H. & STACEY, D. (2014). Approaches, methods, metrics, measures, and subjectivity in ontology evaluation: A survey. *Semantic Web Journal*, **1**, 1–11. [141](#), [142](#), [283](#), [284](#)
- HOBBS, J.R. & PAN, F. (2006). Time ontology in owl. *W3C working draft*, **27**, 133. [136](#)
- HORROCKS, I., PATEL-SCHNEIDER, P.F., BOLEY, H., TABET, S., GROSOFF, B., DEAN, M. *et al.* (2004). Swrl: A semantic web rule language combining owl and ruleml. *W3C Member submission*, **21**, 1–31. [67](#), [198](#)
- IMRAN-DAUD, M., SÁNCHEZ, D. & VIEJO, A. (2016). Ontology-based access control management: Two use cases. In *Proceedings of the 8th International Conference on Agents and Artificial Intelligence (ICAART), Italy*, 244–249. [83](#), [84](#), [85](#), [273](#)
- IQBAL, R., MURAD, M.A.A., MUSTAPHA, A., SHAREF, N.M. *et al.* (2013). An analysis of ontology engineering methodologies: A literature review. *Research journal of applied sciences, engineering and technology*, **6**, 2993–3000. [125](#)

BIBLIOGRAPHY

- JAJODIA, S., SAMARATI, P. & SUBRAHMANIAN, V. (1997). A logical language for expressing authorizations. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy, USA*, 31–42, IEEE. [82](#)
- JAVED, Y., NORRIS, T. & JOHNSTON, D. (2011). Ontology-based inference to enhance team situation awareness in emergency management. In *Proceedings of the 8th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Portugal*, 1–9. [27](#), [28](#), [70](#), [74](#)
- JENA, A. (2014). Apache jena fuseki. *The Apache Software Foundation*. [166](#), [221](#)
- JONES, D., BENCH-CAPON, T. & VISSER, P. (1998). Methodologies for ontology development. In *Proceedings of the 15th IFIP World Computer Congress, Poland*, 1–14. [68](#), [270](#)
- JONES, M., CAMPBELL, B. & MORTIMORE, C. (2015). Json web token (jwt) profile for oauth 2.0 client authentication and authorization grants. Retrieved from <https://tools.ietf.org/html/rfc7523> (accessed 12 July 2020). [188](#), [294](#)
- KAGAL, L. (2002). Rei: A policy language for the me-centric project. Tech. rep., HP Laboratories. [82](#)
- KAGAL, L., FININ, T. & JOSHI, A. (2003). A policy language for a pervasive computing environment. In *Proceedings of the IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Italy*, 63–74, IEEE. [82](#)
- KARRAY, M.H., CHEBEL-MORELLO, B. & ZERHOUNI, N. (2012). A formal ontology for industrial maintenance. *Applied ontology*, **7**, 269–310. [68](#), [69](#), [270](#)
- KIRrane, S., MILEO, A. & DECKER, S. (2017). Access control and the resource description framework: A survey. *Semantic Web*, **8**, 311–352. [82](#)
- KIRSCH-PINHEIRO, M., GENSEL, J. & MARTIN, H. (2004). Representing context for an adaptative awareness mechanism. In *International Conference on Collaboration and Technology, Costa Rica*, 339–348, Springer. [27](#)
- KNOBLICH, G. & SEBANZ, N. (2006). The social nature of perception and action. *Current Directions in Psychological Science*, **15**, 99–104. [250](#)

- KONSTANTOPOULOS, S., PALIOURAS, G. & CHATZINOTAS, S. (2006). Share-ods: an ontology data service for search and rescue operations. In *Hellenic Conference on Artificial Intelligence, Greece*, 525–528, Springer. [44](#), [49](#), [50](#), [66](#), [215](#), [216](#)
- KONSTANTOPOULOS, S., POTTEBAUM, J., SCHON, J., SCHNEIDER, D., WINKLER, T., PALIOURAS, G. & KOCH, R. (2008). Ontology-based rescue operation management. In *International Workshop on Mobile Information Technology for Emergency Response, Germany*, 112–121, Springer. [44](#), [49](#), [50](#), [215](#), [216](#)
- KOUGIAS, I., SEREMETIS, L. & KALOGERAS, D. (2015). Occurrent vs continuant business enterprise: an ontological approach. In *In the 4th International Conference on Quantitative and Qualitative Methodologies in the Economic and Administrative Sciences, Greece*. [135](#)
- KROGSTIE, J., SINDRE, G. & JØRGENSEN, H. (2006). Process models representing knowledge for action: a revised quality framework. *European Journal of Information Systems*, **15**, 91–102. [99](#)
- KULYK, O., VAN DER VEER, G. & VAN DIJK, B. (2008). Situational awareness support to enhance teamwork in collaborative environments. In *Proceedings of the 15th European conference on Cognitive ergonomics: the ergonomics of cool interaction, Portugal*, 1–5. [24](#)
- LA DDSC ET LA DHOS (2009). Référentiel commun : Organisation du secours à personne et de l'aide médicale urgente. [39](#), [91](#), [274](#)
- LABBA, C., SALAH, N.B. & SAOUD, N.B.B. (2017). An agent-based meta-model for response organization structures. In *International Conference on Information Systems for Crisis Response and Management in Mediterranean Countries, Greece*, 154–167, Springer. [94](#), [275](#)
- LAMBERT, G., FONTAINE, B., MONNERET, M. & MADANI, R.M. (2019). How to build an innovative c2 system supporting individual-centric emergency needs? In *Proceedings of the 16th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Spain*, 327–337. [6](#), [47](#), [49](#), [50](#), [215](#), [216](#)

BIBLIOGRAPHY

- LASSILA, O. & MCGUINNESS, D. (2001). The role of frame-based representation on the semantic web. *Linköping Electronic Articles in Computer and Information Science*, **6**, 2001. [64](#)
- LAWSON, T. (2004). A conception of ontology. *Mimeograph, University of Cambridge*. [60](#)
- LI, N., YANG, Z., GHAHRAMANI, A., BECERIK-GERBER, B. & SOIBELMAN, L. (2014). Situational awareness for supporting building fire emergency response: Information needs, information sources, and implementation requirements. *Fire safety journal*, **63**, 17–28. [32](#), [35](#)
- LI, X., LIU, G., LING, A., ZHAN, J., AN, N., LI, L. & SHA, Y. (2008). Building a practical ontology for emergency response systems. In *Proceedings of the 2008 international conference on computer science and software engineering, China*, vol. 4, 222–225, IEEE. [65](#), [73](#), [75](#), [144](#), [145](#)
- LIEBERMAN, H., PATERNO, F. & WULF, V. (2006). *End User Development. Human-Computer Interaction Series, 9th Edition*. Springer. [79](#)
- LIMBU, M., WANG, D., KAUPPINEN, T. & ORTMANN, J. (2012). Management of a crisis (moac) vocabulary specification. Retrieved from <http://observedchange.com/moac/ns/> (accessed 13 January 2021). [73](#), [75](#)
- LORD, P. (2011). Components of an ontology. Retrieved from <http://ontogenesis.knowledgeblogger.org/> (accessed 15 September 2020). [66](#)
- LUDWIG, T., REUTER, C. & PIPEK, V. (2013). What you see is what i need: Mobile reporting practices in emergencies. In *Proceedings of the 13th European Conference on Computer Supported Cooperative Work, Cyprus*, 181–206, Springer. [44](#), [49](#), [50](#), [215](#), [216](#)
- MACÍAS, J.A. & CASTELLS, P. (2007). Providing end-user facilities to simplify ontology-driven web application authoring. *Interacting with Computers*, **19**, 563–585. [79](#), [80](#)
- MACÍAS, J.A., PUERTA, Á.R. & CASTELLS, P. (2006). Model-based user interface reengineering. In *Proceedings of the 5th International Conference on Human Computer Interaction, Spain*, 155–162, Springer. [79](#)

- MAGRO, D. & GOY, A. (2012). A core reference ontology for the customer relationship domain. *Applied Ontology*, **7**, 1–48. [65](#), [136](#)
- MAJOR, R.H. (1859). *Early Voyages to Terra Australis, Now Called Australia*. Hakluyt society. [4](#)
- MALLEK, S., SAUVAGNARGUES, S., TENA-CHOLLET, F., CHARREL, B. & ARNAUD, I. (2016). Contribution to the definition of a new type of more technological ambulance: Use case of french civil security ambulances. *Open Journal of Safety Science and Technology*, **6**, 126–142. [5](#), [37](#), [45](#), [49](#), [50](#), [215](#), [216](#), [261](#), [267](#)
- MARTIN, E., NOLTE, I. & VITOLO, E. (2016). The four cs of disaster partnering: communication, cooperation, coordination and collaboration. *Disasters*, **40**, 621–643. [5](#)
- MASMOUDI, M., KARRAY, M.H., LAMINE, S.B.A.B., ZGHAL, H.B. & ARCHIMEDE, B. (2020). Memon: Modular environmental monitoring ontology to link heterogeneous earth observed data. *Environmental Modelling & Software*, **124**, 104581. [64](#), [65](#), [125](#), [134](#), [136](#)
- MCBRIDE, B. (2004). The resource description framework (rdf) and its vocabulary description language rdfls. In *Handbook on ontologies*, 51–65, Springer. [67](#)
- MCDANIEL, S.E. & BRINCK, T. (1997). Awareness in collaborative systems: a chi 97 workshop. *ACM Special Interest Group on Computer-Human Interaction*, **29**, 68–71. [19](#)
- MCINNERNEY, J.M. & ROBERTS, T.S. (2009). Collaborative and cooperative learning. In *Encyclopedia of Distance Learning, Second Edition*, 203–214, IGI Global. [2](#)
- MEISSNER, A., WANG, Z., PUTZ, W. & GRIMMER, J. (2006). Mikobos-a mobile information and communication system for emergency response. In *Proceedings of the 3rd International Conference on Information Systems for Crisis Response and Management (ISCRAM), Belgium*, 92–101. [43](#), [49](#), [50](#), [215](#), [216](#)
- MIKA, P. (2005). Ontologies are us: A unified model of social networks and semantics. In *International semantic web conference, Ireland*, 522–536, Springer. [84](#)

BIBLIOGRAPHY

- MIZOGUCHI, R. (2004). Tutorial on ontological engineering part 2: Ontology development, tools and languages. *New Generation Computing*, **22**, 61–96. [68](#), [69](#), [125](#), [270](#)
- MIZOGUCHI, R., IKEDA, M., SETA, K. & VANWELKENHUYSEN, J. (1995). Ontology for modeling the world from problem solving perspectives. In *Proceedings of the IJCAI-95 Workshop on Basic Ontological Issues in Knowledge Sharing, Sweden*, 1–12. [69](#), [72](#)
- MOHD ALI, M., YANG, R., ZHANG, B., FURINI, F., RAI, R., OTTE, J.N. & SMITH, B. (2020). Enriching the functionally graded materials (FGM) ontology for digital manufacturing. *International Journal of Production Research*, **58**, 1–18. [136](#)
- MONARES, Á., HERSKOVIC, V., SUÁREZ, D., IBARRA, M., OCHOA, S.F. & PINO, J.A. (2011a). Increasing shared information availability during urban emergency responses. In *Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Switzerland*, 677–684, IEEE. [44](#), [49](#), [50](#), [215](#), [216](#)
- MONARES, Á., OCHOA, S.F., PINO, J.A., HERSKOVIC, V., RODRIGUEZ-COVILI, J. & NEYEM, A. (2011b). Mobile computing in urban emergency situations: Improving the support to firefighters in the field. *Expert systems with applications*, **38**, 1255–1267. [44](#), [49](#), [50](#), [215](#), [216](#)
- MOROSOFF, P., RUDNICKI, R., BRYANT, J., FARRELL, R. & SMITH, B. (2015). Joint doctrine ontology: a benchmark for military information systems interoperability. In *Proceedings of the 10th International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS), USA*. [136](#)
- MOTIK, B., PATEL-SCHNEIDER, P.F., PARSIA, B., BOCK, C., FOKOUE, A., HAASE, P., HOEKSTRA, R., HORROCKS, I., RUTTENBERG, A., SATTLER, U. *et al.* (2009). OWL 2 web ontology language: Structural specification and functional-style syntax. *W3C recommendation*, **27**, 159. [67](#)
- MUNIR, K. & ANJUM, M.S. (2018). The use of ontologies for effective knowledge modelling and information retrieval. *Applied Computing and Informatics*, **14**, 116–126. [67](#), [140](#)

- MUNKVOLD, B.E., RADIANTI, J., RØD, J.K., OPACH, T., SNAPRUD, M., PILEMALM, S. & BUNKER, D. (2019). Sharing incident and threat information for common situational understanding. In *Proceedings of the 16th International Conference on Information Systems for Crisis Response and Management (IS-CRAM), Spain*. **3**, 6, 31
- MUSEN, M.A. (2015). The protégé project: a look back and a look forward. *AI matters*, **1**, 4–12. [140](#), [283](#)
- MUTONGI, C. (2016). Revisiting data, information, knowledge and wisdom (dikw) model and introducing the green leaf model. *IOSR Journal of Business and Management (IOSR-JBM)*, **18**, 66–77. [57](#)
- NOMADEEC FRANCE (2019). Nomadeec mobile telemedicine. Retrieved from <http://nomadeec.com/telemedecine-urgence/> (accessed 24 May 2019). [45](#), [49](#), [50](#), [215](#), [216](#)
- NORRI-SEDERHOLM, T., JOENSUU, M. & HUHTINEN, A.M. (2017). Ensuring information flow and the situation picture in public safety organisations' situation centres. In *Proceedings of the 16th European Conference on Cyber Warfare and Security, Ireland*, 267–273. [25](#)
- NOWELL, B. & STEELMAN, T. (2015). Communication under fire: the role of embeddedness in the emergence and efficacy of disaster response communication networks. *Journal of Public Administration Research and Theory*, **25**, 929–952. [5](#)
- NOY, N.F. & HAFNER, C.D. (1997). The state of the art in ontology design: A survey and comparative review. *AI magazine*, **18**, 53–53. [128](#), [281](#)
- NUNAVATH, V. & PRINZ, A. (2015). Norwegian emergency management process by using business process modeling notation. In *Proceedings of the 8th IADIS International Conference on Information Systems 2015, Portugal*. **36**, [101](#), [277](#)
- NUNAVATH, V., PRINZ, A., COMES, T. & RADIANTI, J. (2013). Ontology of emergency shared situation awareness and crisis interoperability. In *Proceedings of the Norwegian Conference for IT Use in Organisations, Norway*, 159–162, IEEE. **9**, [38](#), [263](#)

BIBLIOGRAPHY

- NUNAVATH, V., PRINZ, A., COMES, T. & RADIANTI, J. (2016). Representing fire emergency response knowledge through a domain modelling approach. In *Norsk konferanse for organisasjoners bruk av IT, Norway*, vol. 24. [72](#), [73](#), [75](#)
- OBERLE, D., GRIMM, S. & STAAB, S. (2009). An ontology for software. In *Handbook on ontologies*, 383–402, Springer. [76](#)
- OH, S. & PARK, S. (2003). Task–role-based access control model. *Information systems*, **28**, 533–562. [193](#)
- OLIVESI, S. (2014). *Sciences de l'information et de la communication: objets, savoirs, discipline*. Presses universitaires de Grenoble. [31](#)
- ÖZACAR, T., ÖZTÜRK, Ö. & ÜNALIR, M.O. (2011). Anemone: An environment for modular ontology development. *Data & Knowledge Engineering*, **70**, 504–526. [133](#), [282](#)
- PARK, J., SUNG, K. & MOON, S. (2008). Developing graduation screen ontology based on the methontology approach. In *4th International Conference on Networked Computing and Advanced Information Management, Korea*, vol. 2, 375–380, IEEE. [139](#), [283](#)
- PAULHEIM, H. (2009). Ontologies for user interface integration. In *International Semantic Web Conference, USA*, 973–981, Springer. [76](#)
- PAULHEIM, H. & PROBST, F. (2010). Ontology-enhanced user interfaces: A survey. *International Journal on Semantic Web and Information Systems (IJSWIS)*, **6**, 36–59. [76](#)
- PAULHEIM, H. & PROBST, F. (2011). A formal ontology on user interfaces yet another user interface description language. In *2nd Workshop on Semantic Models for Adaptive Interactive Systems (SEMAIS), USA*. [76](#), [81](#), [147](#)
- PEASE, A., NILES, I. & LI, J. (2002). The suggested upper merged ontology: A large ontology for the semantic web and its applications. In *Working notes of the AAAI workshop on ontologies and the semantic web*, vol. 28, 7–10. [64](#), [134](#)
- PEASE, A., FELLBAUM, C. *et al.* (2010). Formal ontology as interlingua: The sumo and wordnet linking project and global wordnet. *Computer Science*, **3**. [136](#)

- PINTO, H.S. & MARTINS, J.P. (2004). Ontologies: How can they be built? *Knowledge and information systems*, **6**, 441–464. [69](#), [125](#), [270](#)
- PORTELLI, L., SABATINI, M. & GROGAN, P.T. (2019). Ontology development for knowledge-driven distributed space mission systems engineering. In *AIAA Science and Technology Forum and Exposition (SciTech), USA*, 1032. [134](#)
- PUŽAR, M. (2010). *Towards Secure and Reliable Information Sharing in Emergency and Rescue Operations*. Ph.D. thesis, University of Oslo, Norway. [4](#), [5](#)
- RAJE, S., DAVULURI, C., FREITAS, M., RAMNATH, R. & RAMANATHAN, J. (2012). Using ontology-based methods for implementing role-based access control in cooperative systems. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing, Italy*, 763–764. [83](#), [85](#)
- RASTIER, F. (1995). Le terme: entre ontologie et linguistique. *La banque des mots*, **7**, 35–65. [58](#)
- RICHARD-HIBON, A. & BRAUN, F. (2009). Organisation du secours à personne et de l'aide médicale urgente: Référentiel commun samu-sdis. *Médecine d'urgence (Paris)*, **31**, 89–92. [91](#), [274](#)
- ROBERTS, D.D. (1992). The existential graphs. *Computers & Mathematics with Applications*, **23**, 639–663. [59](#)
- ROGER, P. & MARTIN, L. (2018). Psychological and behavioural responses to cbrn disasters: Implications for emergency response, community, and business continuity. Retrieved from <https://martinlea.com/report-psychological-and-behavioural-responses-to-disasters/> (accessed 14 January 2021). [5](#)
- RUDNICKI, R. (2017). An overview of the common core ontologies. Tech. rep., CUBRC. [71](#), [136](#), [137](#)
- SALMON, P.M., STANTON, N.A., WALKER, G.H., BABER, C., JENKINS, D.P., MCMASTER, R. & YOUNG, M.S. (2008). What really is going on? review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science*, **9**, 297–323. [19](#), [23](#)

BIBLIOGRAPHY

- SALO-LEE, L. (2006). Intercultural competence in research and practice: Challenges of globalization for intercultural leadership and team work. In *Aspects of intercultural dialogue*, 79–92. [30](#)
- SANDHU, R.S., COYNE, E.J., FEINSTEIN, H.L. & YOUMAN, C.E. (1996). Role-based access control models. *Computer*, **29**, 38–47. [81](#), [149](#), [192](#)
- SANTOS, L.S., SICILIA, M.A. & GARCIA-BARRIOCANAL, E. (2019). Ontology-based modeling of effect-based knowledge in disaster response. *International Journal on Semantic Web and Information Systems (IJSWIS)*, **15**, 102–118. [72](#), [75](#)
- SAOUTAL, A. (2015). *Amélioration de l'awareness informationnelle dans la collaboration inter-organisations pendant la gestion de crise*. Ph.D. thesis, University of Technology of Troyes, France. [9](#), [20](#), [31](#), [263](#)
- SAOUTAL, A., CAHIER, J.P. & MATTA, N. (2014). Modelling the communication between emergency actors in crisis management. In *International Conference on Collaboration Technologies and Systems (CTS), USA*, 545–552, IEEE. [2](#), [35](#), [36](#), [94](#), [275](#)
- SAPAUT, D. (2011). Création du bataillon de sapeurs pompiers de paris. Retrieved from <https://francearchives.fr/commemo/recueil-2011/39845> (accessed 12 May 2020). [4](#)
- SCHMIDT, K. (2002). The problem with ‘awareness’: Introductory remarks on ‘awareness in CSCW’. *Computer Supported Cooperative Work (CSCW)*, **11**, 285–298. [2](#), [27](#)
- SCHMITZ, J., BLECHERT, J., KRÄMER, M., ASBRAND, J. & TUSCHENCAFFIER, B. (2012). Biased perception and interpretation of bodily anxiety symptoms in childhood social anxiety. *Journal of Clinical Child & Adolescent Psychology*, **41**, 92–102. [30](#), [31](#)
- SCHOENING, J.R., DUFF, D.K., HINES, D.A., RISER, K.M., PHAM, T., STOLOVY, G.H., HOUSER, J., RUDNICKI, R., GANGER, R. & JAMES, A. (2015). PED fusion via enterprise ontology. In *International Symposium on Optics, Imaging, And Instrumentation, USA*, vol. 9464, 94–112. [65](#)

- SCHREIBER, A.T., SCHREIBER, G., AKKERMANS, H., ANJEWIERDEN, A., SHADBOLT, N., DE HOOG, R., VAN DE VELDE, W., WIELINGA, B. & SHADBOLT, N.R. (2000). *Knowledge engineering and management: the CommonKADS methodology*. MIT press. 55, 56, 57
- SCHULTZ, D.J. *et al.* (1997). Ieee standard for developing software life cycle processes. *IEEE Std*, 1074–1997. 125
- SCHULZ, S. & BOEKER, M. (2013). Biotoplite: An upper level ontology for the life sciences. evolution, design and application. In *INFORMATIK 2013–Informatik angepasst an Mensch, Organisation und Umwelt*, Gesellschaft für Informatik eV. 134
- SCHÜTTE, F., CASADO, R. & RUBIERA, E. (2013). Solving interoperability issues in cross border emergency operations. In *Proceedings of the 10th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Germany*. 66, 70
- SDIS24 FRANCE (2017). Histoire des sapeurs-pompiers. Retrieved from <https://sdis24.com/le-sdis24/histoire-des-sapeurs-pompiers/> (accessed 12 May 2020). 4
- SEELING, C. & BECKS, A. (2003). Exploiting metadata for ontology-based visual exploration of weakly structured text documents. In *Proceedings on Seventh International Conference on Information Visualization, UK*, 652–657, IEEE. 76
- SEMY, S.K., PULVERMACHER, M.K. & OBRST, L.J. (2004). Toward the use of an upper ontology for us government and us military domains: An evaluation. Tech. rep., MITRE CORP BEDFORD MA. 134, 135
- SÉGURET, F. (2013). Sinus, pour le suivi en temps réel des victimes de catastrophes et des grands événements. Retrieved from <https://www.secourisme.net/spip.php?article607> (accessed 24 May 2019). 46, 49, 50, 215, 216
- SHAHZAD, S.K. (2011). Ontology-based user interface development: User experience elements pattern. *Journal of Universal Computer Science*, **17**, 1078–1088. 76, 77, 81

BIBLIOGRAPHY

- SHAHZAD, S.K., GRANITZER, M. & HELIC, D. (2011). Ontological model driven gui development: User interface ontology approach. In *6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Dhaka*, 214–218, IEEE. 77
- SHANNON, C.E. & WEAVER, W. (1949). *The mathematical theory of communication*. Illinois press, Urbana. 29
- SHIMANSKI, C. (2008). Situational awareness in search and rescue operations. In *International Technical Rescue Symposium*, 1–12. 25
- SMITH, B. (2003). Ontology. In *Blackwell guide to the philosophy of computing and information*, 155–166, Oxford. 61
- SMITH, B. & CEUSTERS, W. (2010). Ontological realism: A methodology for coordinated evolution of scientific ontologies. *Applied ontology*, 5, 139–188. 134
- SMITH, B., ALMEIDA, M., BONA, J., BROCHHAUSEN, M., CEUSTERS, W., COURTOT, M., DIPERT, R., GOLDFAIN, A., GRENON, P. & HASTINGS, J. (2015). Basic formal ontology 2.0: Specification and user’s guide. Tech. rep., National Center for Ontological Research, USA. 135
- SMITH, C. & HAYNE, S.C. (1991). A distributed system for crisis management. In *Proceedings of the Twenty-Fourth Annual Hawaii International Conference on System Sciences, USA*, vol. 3, 72–81, IEEE. 31
- SOWA, J.F. (1987). Semantic networks. *Encyclopedia of Artificial Intelligence*. 59
- SOWA, J.F. (1999). *Knowledge representation: logical, philosophical and computational foundations*. Brooks/Cole Publishing Co. 9, 55, 58, 59, 60, 263, 269
- SOWA, J.F. (2008). Conceptual graphs. *Foundations of Artificial Intelligence*, 3, 213–237. 59
- STANTON, N.A., SALMON, P.M., WALKER, G.H., SALAS, E. & HANCOCK, P.A. (2017). State-of-science: situation awareness in individuals, teams and systems. *Ergonomics*, 60, 449–466. 19

- STEEN-TVEIT, K. & RADIANTI, J. (2019). Analysis of common operational picture and situational awareness during multiple emergency response scenarios. In *Proceedings of the 16th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Spain*. 3, 31
- STEIGENBERGER, N. (2016). Organizing for the big one: A review of case studies and a research agenda for multi-agency disaster response. *Journal of Contingencies and Crisis management*, 24, 60–72. 31
- STENMARK, D. (2001). The relationship between information and knowledge. In *Proceedings of the 24th Information Systems Research Seminar in Scandinavia, Norway*, vol. 24, 11–14. 55, 56
- STUDER, R., BENJAMINS, V.R. & FENSEL, D. (1998). Knowledge engineering: principles and methods. *Data & knowledge engineering*, 25, 161–197. 9, 55, 60, 61, 62, 63, 65, 263, 269
- THOMAS, R.K. (1997). Team-based access control (tmac) a primitive for applying role-based access controls in collaborative environments. In *Proceedings of the second ACM workshop on Role-based access control, USA*, 13–19. 81, 149, 192
- THOMAS, R.K. & SANDHU, R.S. (1993). Towards a task-based paradigm for flexible and adaptable access control in distributed applications. In *Proceedings on the 1992-1993 workshop on New security paradigms, USA*, 138–142. 192
- TOURWÉ, T., TSIPOKOVA, E., GONZÁLEZ-DELEITO, N. & HRISTOSKOVA, A. (2011). Ontology-driven elicitation of multimodal user interface design recommendations. In *23rd Benelux conference on Artificial Intelligence (BNAIC), Belgium*, 8–16. 79
- TPLSYSTEMES FRANCE (2019). Pilot mobile. Retrieved from <https://tplsystemes.com/product/47> (accessed 24 May 2019). 46, 49, 50, 215, 216
- TRUPTIL, S., BÉNABEN, F. & PINGAUD, H. (2010). A mediation information system to help to coordinate the response to a crisis. In *Working Conference on Virtual Enterprises, France*, 173–180, Springer. 36

BIBLIOGRAPHY

- TSIPORKOVA, E., TOURWÉ, T. & GONZÁLEZ-DELEITO, N. (2011). Towards a semantic modelling framework in support of multimodal user interface design. In *IFIP Conference on Human-Computer Interaction, Portugal*, 636–639, Springer. 79
- TSIPORKOVA, E., TOURWÉ, T., GONZÁLEZ-DELEITO, N. & HRISTOSKOVA, A. (2012). Ontology-driven multimodal interface design for an emergency response application. In *Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Canada*, 1–6, Ghent University, Department of Information technology. 79, 81
- VALLS, A., GIBERT, K., SÁNCHEZ, D. & BATET, M. (2010). Using ontologies for structuring organizational knowledge in home care assistance. *International journal of medical informatics*, 79, 370–387. 42, 63, 66, 67, 140
- VAN HARMELEN, F., LIFSCHITZ, V. & PORTER, B. (2008). *Handbook of knowledge representation*. Elsevier. 140
- VAN HEIJST, G., SCHREIBER, A.T. & WIELINGA, B.J. (1997). Using explicit ontologies in kbs development. *International journal of human-computer studies*, 46, 183–292. 59, 64
- VELDE, L.V., CHATZINOTAS, S., LARSON, M., LÖFFLER, J. & PALIOURAS, G. (2005). Interactive 2d–3d digital maps for the support of emergency teams during rescue operations. In *Proceedings of the 12th World Congress on Intelligent Transport Systems, USA*, 1575–1584. 44, 49, 50, 215, 216
- VERBAERE, I. (2013). Pompiers et SAMU un mariage impossible ? Retrieved from <https://www.lagazettedescommunes.com/dossiers/pompiers-et-samu-un-mariage-impossible/> (accessed 15 January 2021). 5, 6
- VILLELA, K., BREINER, K., NASS, C., MENDONÇA, M. & VIEIRA, V. (2014). A smart and reliable crowdsourcing solution for emergency and crisis management. 213–220. 66, 71
- VRANDEČIĆ, D. (2009). Ontology evaluation. In *Handbook on ontologies*, 293–313, Springer. 141, 283
- WATZLAWICK, P., BEAVIN, J.H., JACKSON, D.D. & MORCHE, J. (1972). *Une logique de la communication*. Editions du Seuil Paris. 30

- WEGNER, P. & GOLDIN, D. (1999). Interaction as a framework for modeling. In *Conceptual Modeling*, 243–257, Springer. 99
- WIEGAND, N. & GARCÍA, C. (2007). A task-based ontology approach to automate geospatial data retrieval. *Transactions in GIS*, **11**, 355–376. 65, 74, 75
- WIENER, N. (1949). *Cybernetics or control and communication in the animal and the machine*. Technology Press. 30
- WIIG, K.M. (1994). *Knowledge Management Foundations: Thinking about Thinking-how People and Organizations Represent, Create, and Use Knowledge*. Schema Press. 56
- WILKINSON, C.R. & DE ANGELI, A. (2014). Applying user centred and participatory design approaches to commercial product development. *Design Studies*, **35**, 614–631. 10, 263, 264
- WOLBERS, J. & BOERSMA, K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management*, **21**, 186–199. 31
- WOOLDRIDGE, M., JENNINGS, N.R. & KINNY, D. (2000). The gaia methodology for agent-oriented analysis and design. *Autonomous Agents and multi-agent systems*, **3**, 285–312. 37
- YANG, L., PRASANNA, R. & KING, M. (2009). On-site information systems design for emergency first responders. *Journal of Information Technology Theory and Application (JITTA)*, **10**, 2. 32, 35
- YILDIZ, BURCU (2006). Ontology evolution and versioning. Tech. rep., Vienna University of Technology, Karlsplatz. 142
- YONCACI, İ. (2020). *Development of a road map and emergency help and detection system for disaster search and rescue operations*. Ph.D. thesis, Middle East Technical University, Turkey. 4
- YU, K., WANG, Q. & RONG, L. (2008). Emergency ontology construction in emergency decision support system. In *IEEE International Conference on Service Operations and Logistics, and Informatics, China*, vol. 1, 801–805, IEEE. 65, 72, 74, 144, 145

BIBLIOGRAPHY

- YUAN, E. & TONG, J. (2005). Attributed based access control (ABAC) for web services. In *IEEE International Conference on Web Services (ICWS), USA*, IEEE. [81](#), [149](#)
- ZADE, H., SHAH, K., RANGARAJAN, V., KSHIRSAGAR, P., IMRAN, M. & STARBIRD, K. (2018). From situational awareness to actionability: Towards improving the utility of social media data for crisis response. *Proceedings of the ACM on human-computer interaction*, **2**, 1–18. [7](#), [9](#), [40](#), [41](#)
- ZHANG, Z., ZHOU, Y., CUI, J. & MENG, F. (2011). Modelling the information flows during emergency response. In *2011 19th International Conference on Geoinformatics, China*, 1–5, IEEE. [32](#)
- ZHOU, W. (2008). *Access control model and policies for collaborative environments..* Ph.D. thesis, University of Potsdam, Germany. [81](#), [149](#), [193](#)
- ZHOU, W. & MEINEL, C. (2007). Team and task based rbac access control model. In *2007 Latin American Network Operations and Management Symposium, Brazil*, 84–94, IEEE. [193](#)
- ZINS, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the American society for information science and technology*, **58**, 479–493. [56](#)

Samer CHEHADE

Doctorat : Systèmes SocioTechniques

Année 2021

Conception d'un système de communication personnalisable pour support à l'*awareness* situationnelle

Cette thèse porte sur le problème d'*awareness* et des communications dans les opérations de secours. Nous cherchons à concevoir et à mettre en œuvre un système visant à simplifier les communications dans ces opérations en se basant sur des techniques de représentation sémantique et une personnalisation des usages. Pour être utilisé par les unités opérationnelles, il est essentiel de concevoir un tel système de manière à répondre à leurs besoins. De plus, afin de garantir la confidentialité des informations, il est essentiel d'intégrer des techniques de sécurité. Pour aborder ces aspects, nous proposons une approche pour concevoir les interfaces et les spécifications du système. Cette approche consiste en une méthodologie basée sur cinq étapes. Tout d'abord, nous modélisons les interactions entre les différentes parties sur la base de pratiques opérationnelles. Deuxièmement, nous formalisons ces interactions et connaissances à travers une ontologie d'application. Cette ontologie intègre des concepts liés au domaine du secours, à la conception de systèmes et à la sécurité de l'information. Ensuite, nous présentons une plateforme pour concevoir le système. Basée sur l'ontologie développée, cette plateforme permettra aux utilisateurs finaux du système de définir leurs spécifications et de concevoir leurs interfaces de manière personnalisée. De plus, nous proposons une politique de contrôle d'accès basée sur l'ontologie proposée. Finalement, nous présentons un cas d'usage de la plateforme proposée.

Mots clés : secours aux victimes de catastrophes – systèmes informatiques, mesures de sûreté – systèmes, conception de – représentation des connaissances – prise de conscience.

Designing a Customisable Communication System for Situation Awareness in Rescue Operations

This thesis deals with the problem of awareness and communications in rescue operations. We look forward to designing and implementing a communication system aiming to simplify information sharing in rescue operations based on semantic representation techniques and a customisation of uses. In order to be used by operational units, it is essential to design such a system in a way that meets their practical needs. Moreover, in order to guarantee the privacy of information, it is essential to integrate security techniques in the proposed system. In this consequence, we propose in this thesis a novel approach for defining and designing the system's interfaces and specifications. This approach consists of a five-step methodology. First, we analyse and model communications and interactions between different stakeholders based on practical operations. Secondly, we formalise those interactions and knowledge through an application ontology. This ontology integrates concepts related to the rescue domain, to the design of systems and to information security. Afterwards, we present ontology-based platform for designing the system. Based on the developed ontology, this platform will allow the end-users of the system to define its specifications and design its interfaces in a customised way. Moreover, we propose an access control and rights management policy based on the proposed ontology. Eventually, we present a use case scenario of the proposed platform.

Keywords: disaster relief – electronic data processing departments, security measures – system design – knowledge representation (information theory) – awareness.

Thèse réalisée en partenariat entre :

